# *CONSIGLIO REGIONALE DEL LAZIO*

***Direzione:*** SERVIZIO TECNICO

***Area:*** AREA INNOVAZIONE TECNOLOGICA, TRANSIZIONE AL DIGITALE

# DETERMINAZIONE *(con firma digitale)*

**N.** A01129 **del** 20/12/2022 **Proposta n.** 2486 **del** 14/12/2022

***Oggetto:***

Approvazione Manuale di conservazione e Piano della sicurezza dei sistemi di gestione informatica dei documenti del Consiglio regionale del Lazio

***Proponente:***

| | | |
|---|---|---|
| Estensore | FALCHETTI FRANCESCA MARIA | _____*firma elettronica*_____ |
| Responsabile del procedimento | FALCHETTI FRANCESCA MARIA | _____*firma elettronica*_____ |
| Responsabile dell' Area | | _____ |
| Direttore | IALONGO VINCENZO | _____*firma digitale*_____ |

Firma di Concerto





**Richiesta di pubblicazione sul BUR: NO**

Oggetto: Approvazione Manuale di conservazione e Piano della sicurezza dei sistemi di gestione informatica dei documenti del Consiglio regionale del Lazio.

**IL DIRETTORE**

VISTO lo Statuto, approvato con legge statutaria 11 novembre 2004, n. 1 e successive modifiche e, in particolare l'articolo 24;

VISTA la legge regionale 18 febbraio 2002, n. 6 (Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza ed al personale regionale) e successive modifiche;

VISTO il regolamento di organizzazione del Consiglio regionale, approvato con deliberazione dell'Ufficio di presidenza 29 gennaio 2003, n. 3 e successive modifiche;

VISTA la determinazione 9 febbraio 2022, n. A00138 (Istituzione delle aree presso il Consiglio regionale del Lazio. Revoca della determinazione 2 settembre 2021, n. 107);

VISTA la deliberazione dell'Ufficio di Presidenza n. 20 del 28 febbraio 2022 "Ing. Vincenzo Ialongo. Conferimento dell'incarico di direttore del Servizio "Tecnico";

VISTA la legge 7 agosto 1990, n. 241 (Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi) e successive modifiche;

VISTO il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa) e successive modifiche;

VISTO il decreto legislativo 22 gennaio 2004, n. 42 (Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137) e successive modifiche;

VISTO il decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) e successive modifiche;

VISTE le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dell'Agenzia per l'Italia Digitale (AgID);

VISTA la determinazione della Segreteria generale 3 novembre 2021, n. A00671 con la quale è stato costituito il gruppo di lavoro denominato "Gruppo di lavoro per l'elaborazione delle proposte di Manuale di conservazione e di Piano della sicurezza informatica del sistema di gestione informatica dei documenti", coordinato dal Direttore del Servizio Tecnico, Ing. Vincenzo Ialongo;

VISTA la deliberazione dell'Ufficio di Presidenza 3 agosto 2022, n. 93 (Nomina del responsabile per la conservazione dei documenti informatici del Consiglio regionale del Lazio), con la quale il Direttore del Servizio Tecnico, Ing. Vincenzo Ialongo, è stato nominato responsabile per la conservazione dei documenti informatici del Consiglio regionale del Lazio di cui all'art. 44 del d.lgs. 82/2005 e successive modifiche;

VISTA la proposta del Manuale di conservazione e del Piano della sicurezza informatica dei sistemi di gestione informatica dei documenti del Consiglio regionale del Lazio predisposta dal Gruppo di lavoro suindicato, sulla base della recente normativa in materia e, in particolare, delle citate Linee Guida AGID;

PRESO ATTO della nota prot. n. 26003 del 7 novembre 2022, con la quale il Servizio "Prevenzione della corruzione, Trasparenza" ha trasmesso il parere favorevole del Responsabile della protezione dei dati personali;

RITENUTO di adottare il Manuale di conservazione e il Piano della sicurezza dei sistemi di gestione informatica dei documenti del Consiglio regionale del Lazio di cui all'Allegato A e B;

VISTO il decreto legislativo 14 marzo 2013, n. 33 (Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni) e successive modifiche;

**DETERMINA**

Per i motivi espressi in premessa, che costituiscono parte integrante e sostanziale della presente determinazione

1. di approvare il *Manuale di conservazione* e il *Piano della sicurezza dei sistemi di gestione informatica dei documenti del Consiglio regionale del Lazio* di cui all'Allegato A e B;
2. di trasmettere la presente determinazione ai Direttori dei Servizi;
3. di pubblicare la presente determinazione sul sito istituzionale del Consiglio regionale del Lazio, nella sezione "Amministrazione trasparente", sottosezione "Provvedimenti", pagina "Provvedimenti dirigenziali" nonché sul sito intranet del Consiglio stesso nella sezione "Gestione documentale".

*Ing. Vincenzo Ialongo*

CONSIGLIO
REGIONALE
DEL LAZIO



# Manuale di Conservazione del Consiglio regionale del Lazio

**EMISSIONE DEL DOCUMENTO**

| Azione | Data | Nominativo | Funzione |
|---|---|---|---|
| *Redazione* | Agosto 2022 | - | Gruppo di Lavoro giusta determinazione della Segreteria generale n. A00671 del 03.11.2021 |
| *Supervisione* | Agosto 2022 | Ing. Vincenzo Ialongo | Responsabile per la conservazione dei documenti informatici del CRL |
| *Approvazione* | | | |

**REGISTRO DELLE VERSIONI**

| N°Ver/Rev/Bozza | Data emissione | Modifiche apportate | Osservazioni |
|---|---|---|---|
| 1.0 | 29.07.2022 | Prima versione. Bozza. | |
| 1.1 | 31.08.2022 | Integrazioni apportate a seguito della nomina del Responsabile per la conservazione dei documenti informatici del CRL – Deliberazione UdP n. 93 del 03.08.2022 e revisione generale. | |

# Sommario

# 1 RIFERIMENTI NORMATIVI E TERMINOLOGIA

[1] DPCM 3 dicembre 2013 recante "*Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*"

[2] Decreto legislativo 7 marzo 2005, n. 82 - *Codice dell'amministrazione digitale* e ss.mm.ii.

[3] Decreto legislativo 22 gennaio 2004, n. 42 – *Codice dei beni culturali e del paesaggio* e ss.mm.ii. *-bis, 23 -ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*".

*[4]* Decreto legislativo 30 giugno 2003, n. 196 - *Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.*

[5] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[6] LEGGE 7 agosto 1990, n. 241 - *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*.

[7] DECRETO DEL PRESIDENTE DELLA REPUBBLICA 28 dicembre 2000, n. 445 - *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*.

*[8]* Piano Triennale per l'informatica nella Pubblica Amministrazione (https://pianotriennale-ict.italia.it/). [9] Decreto legislativo 14 marzo 2013, n. 33 - *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*.

Ai fini del presente documento, si intendono:

● Ente, Amministrazione, Consiglio: Consiglio regionale del Lazio;

● Titolare, Produttore, Ente Produttore: Consiglio regionale del Lazio;

● Conservatori: i soggetti esterni al Consiglio regionale del Lazio che svolgono attività di conservazione dei documenti informatici, ovvero la Regione Emilia-Romagna tramite il suo Servizio di conservazione (ParER) ed InfoCert S.p.A.;

● Manuale, Manuale di conservazione: il presente documento;

● Manuale di gestione: il Manuale di gestione del flusso documentale e del protocollo informatico del Consiglio regionale del Lazio, approvato con Determinazione n. A00071 del 26 febbraio 2021;

● Manuale di conservazione dei Conservatori: il Manuale di conservazione della Regione Emilia-Romagna e di InfoCert

● ParER: Polo Archivistico Regionale, struttura che gestisce il servizio di conservazione della Regione Emilia-Romagna;

● InfoCert: soggetto conservatore;

● Responsabile dell'ufficio competente in materia di gestione documentale: soggetto interno al Consiglio regionale del Lazio responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del decreto del Presidente della Repubblica 28 dicembre

2000, n. 445 e ss.mm.;

● Responsabile della conservazione: soggetto interno al Consiglio regionale del Lazio, che definisce e attua le politiche complessive del Sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia;

● Responsabile del Servizio di Conservazione: soggetto interno al Conservatore che coordina il processo di conservazione, in possesso dei requisiti professionali individuati da AgID;

● Servizio di conservazione: servizio affidato ai Conservatori;

● Sistema di conservazione, Sistema: insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'articolo 44, comma 1, del decreto legislativo 07 marzo 2005, n. 82, e successive modifiche e integrazioni.

# 2 SCOPO E AMBITO DEL DOCUMENTO

Il manuale di conservazione, come previsto dal paragrafo 4.6 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici emanate da AGID, è un documento informatico che deve, tra l'altro, illustrare dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione del Consiglio regionale del Lazio.

Quest'ultimo, nella qualità di **Soggetto produttore**, si avvale di due servizi di Conservazione affidati a InfoCert S.p.A. per quanto riguarda i registri giornalieri di protocollo, trasmissione e ricezione atti legislativi tra Giunta e Consiglio, Contratti pubblici informatici, PEC e Regione Emilia Romagna (tramite il Polo archivistico dell'Emilia Romagna), per quanto riguarda le determinazioni contenuti sul nuovo sistema amministrativo contabile; ParER e InfoCert, svolgono la funzione di conservazione e realizzano e gestiscono il Processo di Conservazione ai sensi della normativa nazionale.

L'accordo di collaborazione ex art. 15 L. 241/90, tra Consiglio regionale del Lazio e ParER, per l'affidamento in outsourcing del Processo di Conservazione relativo alle tipologie documentali del sistema amministrativo contabile è stato approvato con Delibera di Giunta Regionale n. 484 del 27.7.2021.

Per le altre tipologie documentali attualmente inviate in conservazione il servizio è stato affidato alla società InfoCert S.p.A. con determinazione n. A00213 del 11/03/2022.

La redazione del manuale di conservazione contempera l'assolvimento dell'obbligo normativo con le esigenze concrete del Soggetto produttore.

Il manuale costituisce una guida per gli attori coinvolti nel processo di gestione e di conservazione, per il cittadino e per le imprese: ai primi, per porre in essere le corrette operazioni di gestione e conservazione documentale, agli ultimi due per comprendere le caratteristiche del Sistema di Conservazione documentale e dei processi erogati.

Il manuale descrive, inoltre, il processo, le architetture e le infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del Sistema di Conservazione.

Il manuale integra, per le parti specifiche di competenza del Soggetto produttore e per quanto riguarda i rapporti tra questi e i Conservatori, i *manuali di conservazione dei Conservatori*, reperibili sul sito dell'Agenzia per l'Italia digitale (AgID), alla pagina dedicata ai conservatori accreditati (https://conservatoriqualificati.agid.gov.it/?page_id=276).

Per quanto riguarda le tipologie documentali degli oggetti sottoposti a conservazione, il manuale è integrato

con appositi Disciplinari tecnici e Schede di attivazione concordati tra Soggetto produttore e Conservatori, che definiscono le specifiche operative e le modalità di descrizione e di versamento nei Sistemi di Conservazione digitale dei documenti informatici, relativamente alle varie tipologie documentali.

# 3 MODELLO ORGANIZZATIVO DELLA CONSERVAZIONE: RUOLI E RESPONSABILITÀ

## 3.1 MODELLO ORGANIZZATIVO

Il Soggetto produttore è il Titolare delle unità documentarie informatiche poste in conservazione e, attraverso il proprio Responsabile della Conservazione, definisce e attua le politiche complessive del Sistema di Conservazione governandone la gestione con piena responsabilità ed autonomia.

Ancora, il Soggetto produttore può procedere alla conservazione dei documenti informatici sulla base del modello in *outsourcing*, che prevede l'affidamento parziale o totale, nel rispetto della disciplina vigente, del Processo di Conservazione a soggetti pubblici o privati ai sensi dell'art. 34, comma 1-bis del Decreto legislativo 7 marzo 2005, n. 82.

Tanto premesso, il modello organizzativo individuato dal Consiglio regionale del Lazio per la gestione del Processo di Conservazione delle unità documentarie informatiche ad esso facenti capo è quello in outsourcing e si concretizza con l'affidamento della gestione del Servizio di Conservazione ai Conservatori secondo quanto previsto dalla normativa in materia.

Nel modello adottato il Soggetto produttore, di intesa con il Titolare del trattamento dei dati personali e con il Responsabile della protezione dei dati, si fa carico della distribuzione dell'informazione ai soggetti aventi diritto di accesso a quest'ultima, nel rispetto delle norme in materia di protezione dei dati personali, così come schematizzato nella figura seguente ed in conformità al modello funzionale OAIS (https://www.iso.org/standard/57284.html).

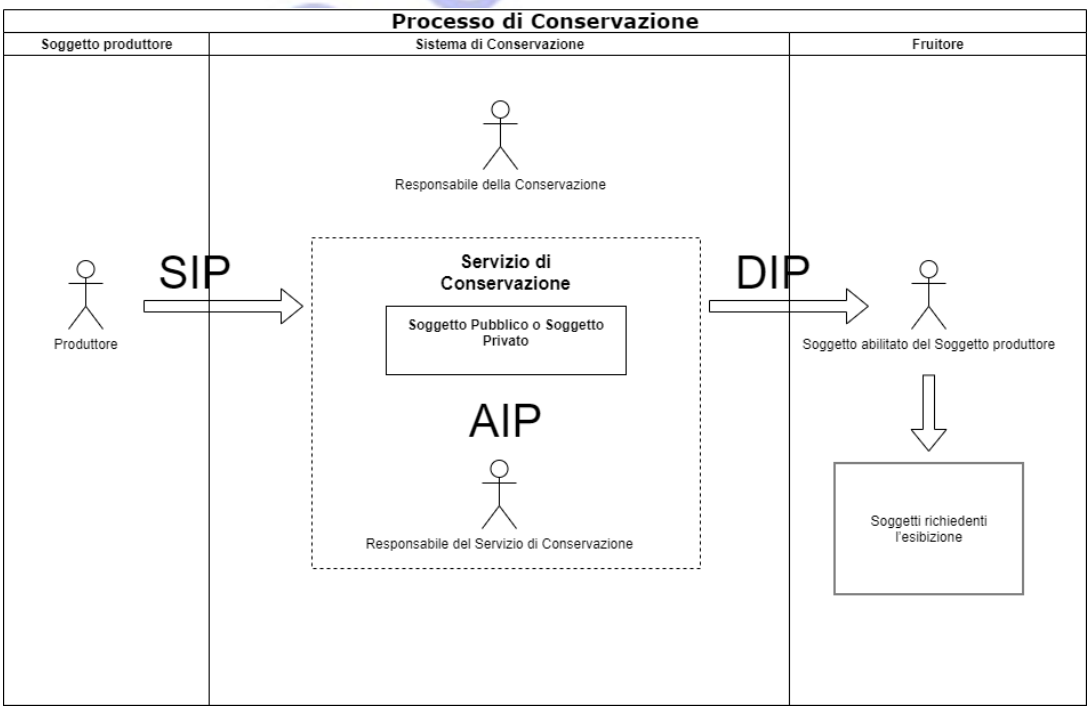


*Figura 3.1 – Processo di conservazione*

Dove:

- **SIP** = Submission Information Package (**Pacchetto di Versamento**).
- **AIP** = Archivial Information Package (**Pacchetto di Archiviazione**).
- **DIP** = Dissemination information Package (**Pacchetto di Distribuzione**). Il

modello organizzativo prevede la presenza delle seguenti figure:

- Per il Soggetto produttore:
  - Responsabile della Conservazione;
  - Responsabile dell'ufficio competente in materia di gestione documentale;
  - Titolare del trattamento dei dati personali;
  - Responsabile della protezione dei dati;
- Per i Conservatori si rimanda al manuale di conservazione degli stessi.

A queste figure, si affiancano quelle relative al Ministero per i Beni e le Attività culturali (MiBAC), nella qualità di organismo di tutela e vigilanza, in relazione a quanto previsto dalla normativa di settore.

## 3.2 SOGGETTO PRODUTTORE

Il Consiglio regionale del Lazio è il Soggetto produttore, Titolare delle unità documentarie informatiche da conservare, insieme agli opportuni metadati, in continuità con il processo di gestione documentale, iniziato nella fase corrente all'interno dell'Ente.

I Conservatori sono stati designati quali responsabili (esterni) del trattamento dei dati personali rispettivamente:

- per ParER , viene designata la Regione Emilia-Romagna (art. 9 dell'accordo di collaborazione richiamato);
- per Infocert, mediante affidamento del procedimento di conservazione "Servizio Legaldoc" da parte del responsabile della Conservazione.

I rapporti tra Soggetto produttore e Conservatori sono altresì disciplinati:

- dal presente manuale,
- dal manuale di conservazione dei Conservatori,
- dai Disciplinari tecnici e dalle scede di attivazione che definiscono gli accordi di versamento per le diverse tipologie documentali oggetto di conservazione.

Al presente manuale sono allegati i Disciplinari tecnici/schede di attivazione, vigenti al momento della sua adozione, che definiscono gli accordi di versamento per le diverse tipologie documentali.

## 3.3 ORGANIGRAMMA

Con riferimento alla fase corrente del processo di gestione documentale, così come previsto dall'art. 4 della L. 7 agosto 1990, n. 241, dall'art. 50, comma 5, del D.P.R. 28 dicembre 2000, n. 445, il Soggetto produttore è organizzato in un'unica Area organizzativa omogenea (AOO), denominata *Consiglio regionale del Lazio* (determinazione dirigenziale n. 274 del 2 aprile 2012), composta dall'insieme di tutti gli Uffici organizzativi di Riferimento (UOR).

L'area organizzativa omogenea è l'insieme di funzioni e di strutture individuate dall'amministrazione cui sono assegnate funzioni omogenee. Essa, pertanto, presenta esigenze di gestione documentale in modo unitario

e coordinato, ai sensi della normativa vigente.
L'Ufficio organizzativo di Riferimento è una unità organizzativa dell'Ente costituita da un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.
Lo schema rappresentato nella Figura 3.2 riassume l'organigramma dell'Ente. La Figura 3.3 schematizza l'organigramma riferito alle sole unità organizzative dell'Ente che prevedono ruoli coinvolti nel Processo di Conservazione.
Per maggiori dettagli inerenti all'organizzazione si rimanda al Manuale di Gestione del Soggetto produttore (DET_A00071_2021.pdf (regione.lazio.it)).

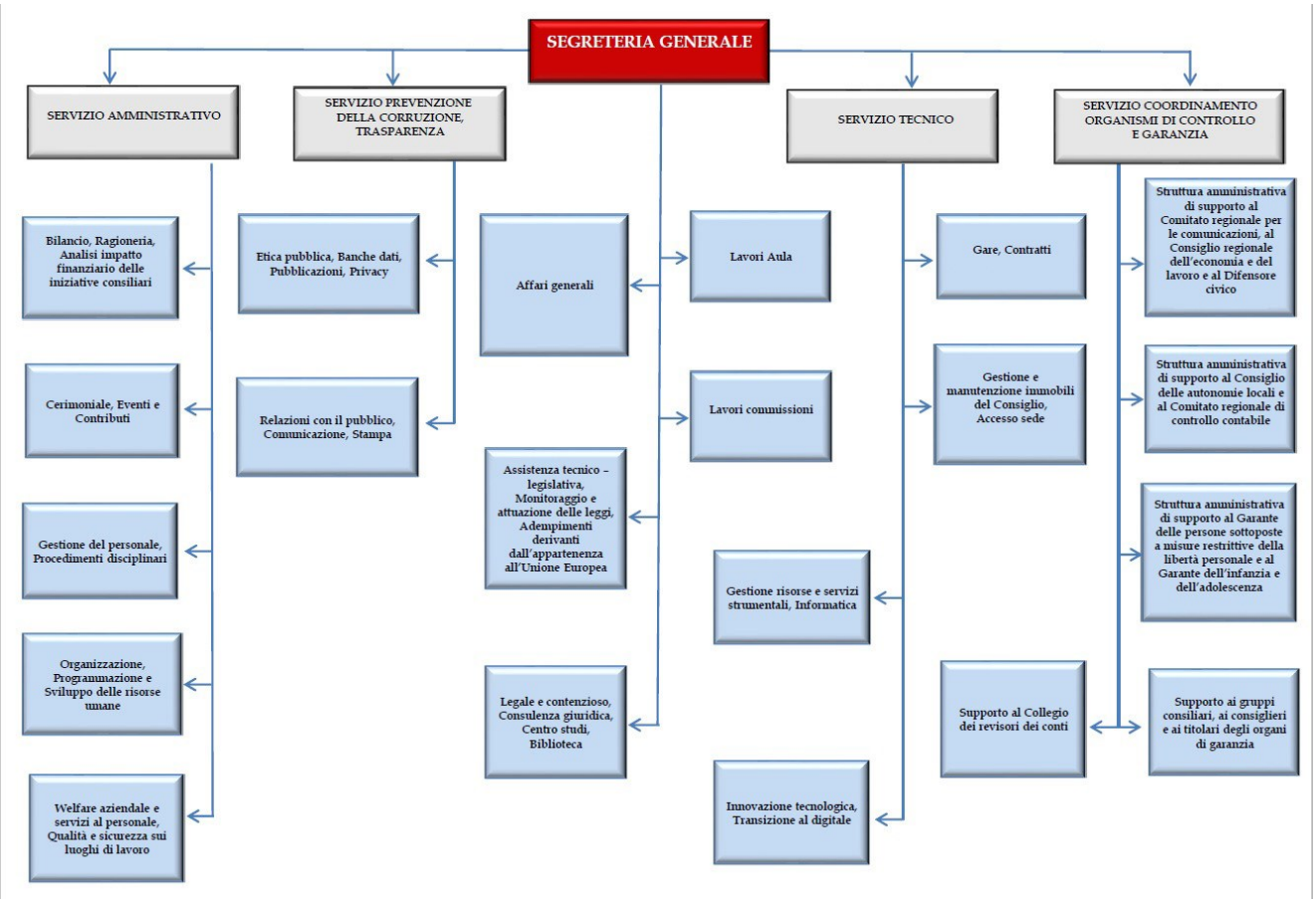


*Figura 3.2 - Organigramma dell'Amministrazione*

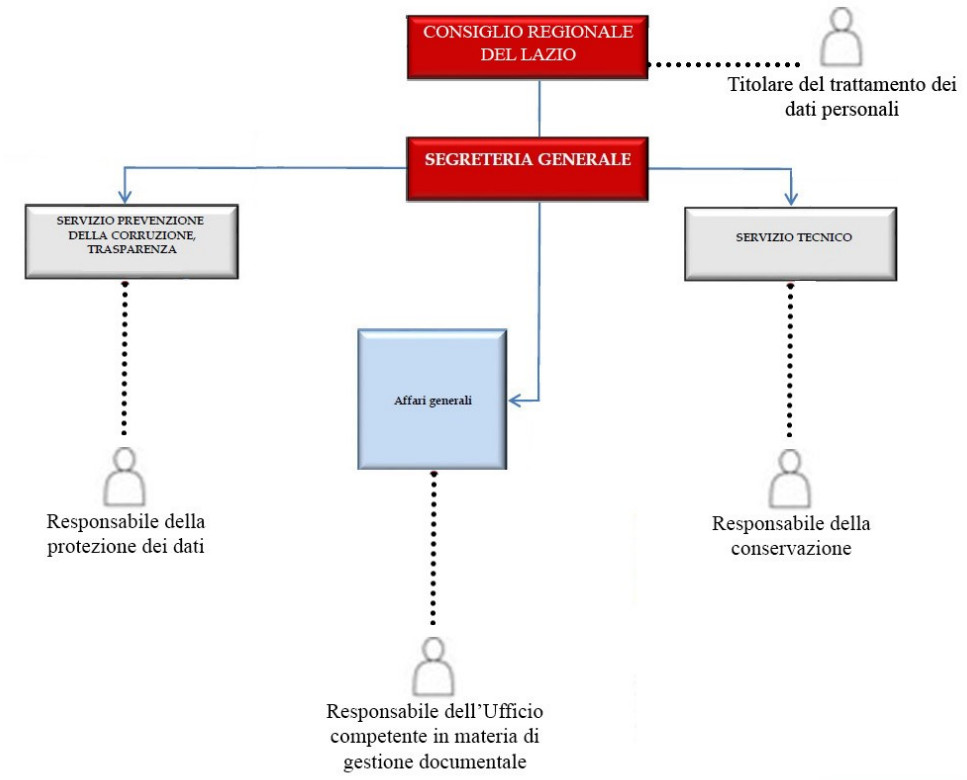


*Figura 3.3 - Organigramma riferito alle sole unità organizzative dell'Amministrazione che prevedono ruoli coinvolti nel processo di conservazione*

Il versamento in conservazione dei documenti informatici gestiti nella fase corrente dalle articolazioni amministrative (AOO e UOR) del Soggetto produttore è effettuato unicamente dal Produttore, laddove non avvenga con processi automatici o venga diversamente specificato nei Disciplinari tecnici.
Le operazioni di recupero dei Pacchetti di Distribuzione sono effettuate dal personale designato dal Soggetto produttore in ciascun UOR della struttura amministrativa e comunicato al Responsabile della Conservazione.
Per quanto riguarda l'organigramma relativo ai Conservatori, si rimanda al manuale di conservazione dei Conservatori.

## 3.4 STRUTTURA ORGANIZZATIVA

Il Sistema di Conservazione delle unità documentarie informatiche e delle unità archivistiche informatiche del Soggetto produttore prevede la collaborazione tra unità organizzative e soggetti interni ed esterni, a cui il Soggetto produttore ha affidato la gestione del Servizio di Conservazione in base all'accordo di collaborazione e ai Disciplinari tecnici, nei quali, per ogni singola tipologia documentale, sono definiti, tra l'altro, i tempi di versamento, i formati e i metadati descrittivi utili a garantire una corretta interazione tra Soggetto produttore e Conservatori.
In virtù di tale affidamento, i Conservatori si impegnano alla conservazione dei documenti trasferiti, assumono la funzione di *Responsabili del Servizio di Conservazione* ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione, e svolgono l'insieme delle

attività elencate nel paragrafo 4.5 delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, in particolare quelle indicate alle lettere a), b), c), d), g), h) e i).
L'esecuzione del Processo di Conservazione avviene sotto la vigilanza del Responsabile della Conservazione, il quale interagisce con il Responsabile del Servizio di Conservazione così come dettagliato in § 3.6.

## 3.5 UTENTE

L'utente è la persona fisica o giuridica, interna o esterna al Sistema di Conservazione, secondo il modello organizzativo adottato, che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Nel modello organizzativo adottato, l'utente finale del Sistema di Conservazione è lo stesso Soggetto produttore che, tramite il proprio personale autorizzato, interagisce con il Servizio di Conservazione per accedere ai documenti per finalità gestionali, amministrative, storiche o per soddisfare le richieste di eventuali soggetti esterni legittimati all'esibizione/accesso alla documentazione (es: amministrazioni/enti pubblici, soggetti privati, aziende, professionisti, cittadini, etc.).
Il Servizio di Conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, ai documenti informatici conservati e consente la produzione di un Pacchetto di Distribuzione direttamente acquisibile dai soggetti abilitati.
Nel ruolo dell'Utente sono definiti gli specifici soggetti autorizzati dal Soggetto produttore che possono accedere esclusivamente ai documenti versati o solo ad alcuni di essi, secondo le regole di visibilità e di accesso concordate tra Soggetto produttore e Conservatori.
L'abilitazione e l'autenticazione di tali operatori avviene in base alle procedure di gestione utenze indicate nel *Piano della sicurezza del sistema di conservazione* dei Conservatori, e nel rispetto delle misure previste dalla vigente normativa in materia di privacy e sicurezza informatica. I Conservatori provvedono a inviare le credenziali di accesso ai diretti interessati.
Più in generale, per quanto attiene al Piano di sicurezza del Sistema di Conservazione, si rimanda al "Piano della sicurezza dei sistemi di gestione informatica dei documenti", allegato al Manuale di Gestione del Soggetto produttore e al Piano della sicurezza del sistema di conservazione dei Conservatori.

## 3.6 RESPONSABILE DELLA CONSERVAZIONE

Il Responsabile della Conservazione è la figura cardine che governa il Processo della Conservazione digitale: è la persona fisica inserita stabilmente nell'organico del Soggetto produttore dei documenti, che definisce e attua le politiche complessive del Sistema di Conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato.
Nel caso di affidamento del Servizio di Conservazione ad un soggetto esterno, il Responsabile della Conservazione del Soggetto produttore delega la funzione di Responsabile del Servizio di Conservazione.
È compito del Responsabile della Conservazione, coadiuvato dal Responsabile del Servizio di Conservazione:

- accertare, con periodicità almeno annuale, la conformità del Processo di Conservazione alla normativa vigente;
- predisporre il manuale di conservazione e curarne l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti;

Al Responsabile del Servizio di Conservazione sono affidate le seguenti specifiche funzioni e competenze:

- definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle

specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;

- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- predispone le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;
- assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza.

Il Responsabile della Conservazione opera d'intesa con il Responsabile del Servizio di Conservazione, con il Responsabile della protezione dati, con il Responsabile del trattamento dati personali (ParER e InfoCert), con il Responsabile della sicurezza del Servizio di Conservazione (ParER e InfoCert) e con il Responsabile dell'ufficio competente in materia di gestione documentale (Consiglio regionale del Lazio).

## 3.7 ORGANISMI DI TUTELA E DI VIGILANZA

Gli archivi e i singoli documenti prodotti dal Consiglio regionale del Lazio sono considerati beni culturali (vedasi l'art. 10, comma 2, lett. b) del Decreto legislativo 22 gennaio 2004, n. 42 – Codice dei beni culturali e del paesaggio e ss.mm.) e sottoposti, pertanto, alle disposizioni di tutela previste nello stesso. Garantire la tutela di archivi e singoli documenti si concretizza negli obblighi conservativi (vedasi art. 30 del citato Codice) che comportano, infatti, "l'obbligo di conservare i propri archivi nella loro organicità e di ordinarli." (art. 30, c. 4 del Decreto legislativo 22 gennaio 2004, n. 42).

Con riferimento agli archivi del Consiglio regionale del Lazio, il rispetto delle disposizioni in ordine alla corretta conservazione è in capo al Ministero per i Beni e le Attività culturali, attraverso la Direzione generale archivi e, in particolare, alla Soprintendenza archivistica e bibliografica del Lazio. Tale ente, infatti, è investito del potere di vigilanza e ispezione ai sensi degli artt. 18 e 19 del Decreto legislativo 22 gennaio 2004, n. 42.

Per quanto riguarda il Sistema di Conservazione del Consiglio regionale del Lazio, la Soprintendenza archivistica e bibliografica del Lazio verifica, in particolare, che il Processo di Conservazione avvenga in modo conforme alla normativa e ai principi di corretta e ininterrotta custodia.

Nel rispetto delle disposizioni normative, il presente manuale verrà inviato alla Soprintendenza archivistica e bibliografica del Lazio.

Il legislatore ha previsto un altro ente che, in materia di conservazione digitale, lavora in parallelo alla Soprintendenza, avendo però un ruolo diverso. L'**Agenzia per l'Italia digitale**, infatti, per quanto concerne i

sistemi di conservazione di archivi e documenti digitali, ha il compito di vigilare sui soggetti diventati Conservatori accreditati. L'attività di vigilanza di AgID riguarda, quindi, il soggetto accreditato e il Sistema di Conservazione nel suo complesso, In materia di sistemi di conservazione e documento informatico, AgID, inoltre, emana Linee guida contenenti regole, standard e guide tecniche, favorendo il coordinamento e la condivisione delle informazioni tra gli enti pubblici.

# 4 ORGANIZZAZIONE DEL SERVIZIO DI CONSERVAZIONE

## 4.1 RESPONSABILITÀ DEL SISTEMA DI CONSERVAZIONE

I Sistemi di Conservazione garantiscono l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli oggetti conservati dal momento della loro presa in carico dal Soggetto produttore, fino all'eventuale scarto, indipendentemente dall'evolversi del contesto tecnologico e organizzativo.
La responsabilità dei Sistemi di Conservazione come soggetti che svolgono il Processo di Conservazione è in capo a ParER e InfoCert.

## 4.2 GESTIONE DEL SISTEMA DI CONSERVAZIONE

Si rimanda al manuale di conservazione dei Conservatori.

### 4.2.1 Organigramma

Si rimanda al manuale di conservazione dei Conservatori.

### 4.2.2 Struttura organizzativa

Si rimanda al manuale di conservazione dei Conservatori.

### 4.2.3 Pubblico ufficiale

Per quanto riguarda ParER: nei casi previsti dalla normativa, il ruolo di pubblico ufficiale è svolto dal Responsabile del servizio ParER in qualità di dirigente dell'ufficio responsabile della conservazione dei documenti, o da altri dallo stesso formalmente designati, quale il Responsabile della Funzione archivistica di conservazione per l'attestazione di conformità all'originale di copie di Documenti informatici conservati.
Per quanto riguarda InfoCert: laddove richiesto dalla natura delle attività, il Responsabile della Conservazione può in autonomia formare copie su diversi supporti dei documenti ottenuti dai pacchetti di distribuzione, anche con l'intervento di un pubblico ufficiale, a garanzia della loro conformità all'originale. Anche il Responsabile del servizio può valutare il coinvolgimento di un pubblico ufficiale, in relazione all'evolversi dei formati e del contesto tecnologico dei sistemi.
Per ulteriori dettagli si rimanda al manuale di conservazione dei Conservatori.

# 5 OGGETTI SOTTOPOSTI A CONSERVAZIONE

## 5.1 DOCUMENTI INFORMATICI E AGGREGAZIONI DOCUMENTALI INFORMATICHE (SERIE E RELATIVI REPERTORI)

I Sistemi di Conservazione acquisiscono, gestiscono, organizzano e conservano documenti informatici, in particolare documenti amministrativi informatici e le loro aggregazioni documentali informatiche, sotto

forma di fascicoli e serie. Ai fini della corretta conservazione nel medio e lungo periodo è indispensabile conoscere la natura degli oggetti informativi complessi, siano essi dei documenti che loro aggregazioni.
All'art. 1, lettera p) del CAD si definisce cosa debba intendersi per documento informatico e, al successivo art. 23-ter, si specifica la particolare categoria di documento informatico rappresentata dal *documento amministrativo informatico* ribadendone la natura di informazione primaria e originale.
Il documento amministrativo informatico è prodotto e memorizzato su di un supporto elettronico durante lo svolgimento di un'attività di carattere amministrativo e, grazie al Sistema di Gestione in cui è stato inserito al momento dell'acquisizione, possiede le opportune caratteristiche di immodificabilità, integrità e staticità, come previsto dalla normativa vigente (vedasi capitolo 2 delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici).
Durante la vita nel Sistema di Gestione corrente, il documento è sottoposto a una serie di azioni (es. protocollazione o registrazione a sistema, classificazione, attribuzione al Responsabile del procedimento, attribuzione al fascicolo, etc.) che ne determinano la posizione logica all'interno dell'archivio così come l'identità: la particolarità e unicità del documento è caratterizzata proprio dalla specifica funzione che esso riveste nello svolgimento dell'attività del Soggetto produttore. Le caratteristiche proprie del documento vengono tradotte in ambito elettronico in metadati: informazioni connesse al documento che consentono, all'interno del Sistema, l'identificazione, la descrizione, la gestione e la conservazione. La normativa prescrive un pacchetto minimo di metadati da associare al documento informatico immodificabile (vedasi Linee Guida sulla formazione, gestione e conservazione dei documenti informatici).
In tal senso risulta fondamentale l'appartenenza del documento al fascicolo. La fascicolazione, oltre a essere un obbligo previsto dalla normativa (art. 41, comma 2 del CAD), è il requisito indispensabile per la corretta gestione del documento all'interno del contesto relazionale che ne determina il significato e l'identità. Fascicolare significa esplicitare la posizione logica del singolo documento all'interno dell'archivio, quindi stabilire esattamente la funzione che il documento svolge. Ad esempio, tutti i documenti che fanno parte del medesimo procedimento appartengono allo stesso fascicolo e vanno tenuti insieme nell'ordine cronologico, cosiddetto ordine di sedimentazione, in base al quale si sono formati; in tal modo si ottiene un fascicolo che contiene la storia del procedimento. Le azioni a cui il documento è soggetto nel corso della propria esistenza sono strettamente determinate dall'appartenenza al fascicolo.
Il passaggio del documento dal Sistema di Gestione al Sistema di Conservazione deve consentire il mantenimento delle caratteristiche del documento di immodificabilità, integrità e staticità, così come deve essere mantenuto il legame significante del documento con il fascicolo al fine di preservare e tramandare, per il periodo necessario, il valore giuridico probatorio, amministrativo e storico.
Le aggregazioni di documenti informatici o di fascicoli informatici sono l'insieme definito e qualificato di documenti riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Il fascicolo rappresenta, quindi, la prima forma di aggregazione determinata e può essere organizzato raccogliendo documenti diversi per formato, natura, contenuto giuridico, ma prodotti nel corso di una specifica attività; oppure raccogliendo documenti della stessa tipologia o qualità o forma, raggruppati quindi in base a criteri estrinseci, e riguardanti contenuti disomogenei.
In particolare, è possibile distinguere tra differenti tipologie di fascicoli (es.: fascicolo di persona, fascicolo di affare, fascicolo di attività, fascicolo procedimentale, fascicolo di fabbricato e fascicolo edilizio).
La distinzione tipologica dei fascicoli deriva dal particolare iter di produzione della documentazione, per cui la catena delle azioni che pongono in essere un insieme di documenti determina anche le modalità con cui i

documenti vengono organizzati e archiviati e dà luogo, nel medio e lungo periodo, al cosiddetto processo di sedimentazione.
I fascicoli, così come particolari tipologie di documenti, creano ulteriori aggregazioni documentali definite serie. Si tratta di articolazioni interne all'archivio createsi sulla base del processo di sedimentazione reso esplicito dall'applicazione del *titolario di classificazione*. Le serie sono funzionali all'individuazione di caratteristiche comuni per documenti o fascicoli, e consentono di conseguenza un'efficiente gestione dei dati oltre a rappresentare un elemento indispensabile della struttura dell'archivio. Dal punto di vista dei fascicoli, le serie si creano rispettando l'articolazione del titolario di classificazione sulla base del quale i singoli fascicoli vengono classificati e inseriti nel repertorio dei fascicoli.
La serie può corrispondere anche al raggruppamento di specifiche tipologie documentali, le quali, quindi, condividono un insieme di caratteristiche omogenee, tradotte in ambito informatico in un set di metadati.

Nell'art. 41, comma 2-ter, del CAD vengono elencate le indicazioni di cui il fascicolo deve essere provvisto per la corretta identificazione e gestione, mentre, il successivo art. 44, esplicitando i requisiti per la gestione e conservazione dei documenti informatici, dichiara che annualmente devono essere trasferiti al Sistema di Conservazione "*i fascicoli e le serie documentarie anche relative a procedimenti non conclusi*". La gestione del fascicolo e delle aggregazioni documentali viene affrontata anche dal paragrafo 3.3 delle Linee Guida AgID.
L'elenco delle tipologie documentali e delle aggregazioni documentali sottoposte a conservazione e versate al Sistema di Conservazione da parte del Produttore è definito nei disciplinari tecnici e le schede di attivazione.
Eventuali variazioni delle condizioni delle tipologie documentali ovvero l'estensione della conservazione ad altre tipologie di documenti, sono individuate dal Produttore, comunicate al Responsabile della Conservazione e definite, con successive note, aggiornando di volta in volta i disciplinari tecnici e le schede di attivazione allegati al presente manuale. Tale aggiornamento è soggetto ad autorizzazione da parte della Soprintendenza Archivistica e Bibliografica del Lazio.

## 5.2 UNITÀ ARCHIVISTICHE E UNITÀ DOCUMENTARIE

Il rapporto tra *unità archivistiche* e *unità documentarie* subisce in ambito informatico una traslazione rispetto alla tradizione archivistica e ciò è dovuto a esigenze gestionali, legate alla specificità dei supporti con cui vengono veicolate le unità informative in ambito informatico.
L'*unità archivistica* in ambito analogico è l'unità base costituita dall'insieme di documenti che condividono determinate caratteristiche identificative, risultato di un processo di produzione, che fanno dell'unità un'aggregazione qualificata e non casuale. In tal senso, l'unità archivistica è il livello di definizione e descrizione dell'aggregazione documentale oltre il quale non è possibile procedere, ossia i documenti che la costituiscono sono elementi che non possiedono un'identità propria se tolti, ad esempio, dal fascicolo, cioè se decontestualizzati. L'unità archivistica nella maggior parte dei casi corrisponde al fascicolo, quindi un insieme di documenti.
In ambito informatico tale rapporto, benché mantenga il rispetto dei principi archivistici, risulta più complesso, poiché l'*unità documentaria* diventa a sua volta un contenitore la cui natura è pre-strutturata sulla base della tipologia di informazioni che deve contenere: si articola in documenti principali, allegati, componenti. Il Consiglio regionale, in qualità di Soggetto produttore, determina la relazione di appartenenza tra i documenti che costituiscono l'unità documentaria e l'unità archivistica, mentre i Conservatori, in un secondo momento, si fanno carico di mantenere stabili, consultabili e contestualizzate nel tempo tali

informazioni, secondo quanto definito nel manuale di conservazione dei Conservatori e nei Disciplinari tecnici e schede di attivazione che integrano il presente documento.

## 5.3 FORMATI

Il formato è l'insieme di informazioni che determina la modalità con cui un oggetto digitale viene creato, memorizzato e riprodotto. Un oggetto digitale è una sequenza di bit fissati con una certa organizzazione fisica su di una memoria. Tale contenuto digitale viene memorizzato e definito come *file*. La possibilità di fruire e utilizzare un file è determinata dalla capacità di rappresentare la sequenza di bit per mezzo di un apposito software che riproduca, sulla base dei codici e delle regole che costituiscono il file stesso, il contenuto e la forma che gli era stata conferita dall'autore.
La corretta conservazione dei documenti nel tempo è determinata anche dalla scelta dei formati idonei a tale scopo. Infatti, un problema di cui è necessario tener conto, è costituito dall'obsolescenza dei formati. Attualmente la soluzione più sicura è adottare, fin dal momento della formazione dei contenuti digitali, formati che abbiano le caratteristiche per fornire le maggiori garanzie in termini di conservazione a lungo termine.

## 5.4 METADATI

Insieme alla scelta dei formati, la definizione dei metadati è un'operazione fondamentale per l'attività conservativa delle memorie digitali a medio e lungo termine.
I metadati sono oggetti da sottoporre a conservazione associati ai documenti informatici, ai documenti amministrativi informatici e ai fascicoli informatici o aggregazioni documentali come stabilito dalle Linee Guida AgID sul documento informatico.
I metadati sono informazioni associate ai dati primari creati e trattati: sono a loro volta dati che descrivono, spiegano, localizzano una risorsa informativa rendendo più semplice il suo recupero, utilizzo e gestione. Metadati sono, ad esempio, il riferimento all'autore o alla tipologia di dato, il riferimento temporale alla creazione o registrazione del dato, la classificazione, etc. Come si può intuire, i metadati associati a una risorsa sono potenzialmente infiniti e, tipicamente, vengono distinti in tre principali categorie:

- *Metadati descrittivi*, descrivono una risorsa con lo scopo di scoprirla ed identificarla;
- *Metadati strutturali*, indicano la struttura di oggetti composti (ad esempio, i capitoli che assemblano le pagine);
- *Metadati amministrativi*, descrivono le informazioni volte a favorire la gestione del file (tipo di file, nome del produttore, riferimento temporale, etc.).

Ad esempio, i dati e i metadati relativi all'oggetto informativo e alle informazioni sulla rappresentazione costituiscono un'unità denominata *contenuto informativo* e in tale forma viene conservata al fine di assicurare la fruibilità e la comprensibilità nel lungo periodo; i metadati descrittivi, invece, che descrivono e identificano le informazioni archiviate, potrebbero essere conservati separatamente in appositi database.
Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici che integrano il presente documento in cui sono definite le specifiche operative e le modalità di descrizione e di versamento nel Sistema di Conservazione digitale delle diverse tipologie documentali oggetto di conservazione, incluse l'individuazione e la gestione dei metadati relativi ai documenti versati nel Sistema di Conservazione.

## 5.5 PACCHETTO INFORMATIVO

Gli oggetti sottoposti a conservazione, siano essi aggregazioni documentali informatiche, documenti informatici, o metadati, sono trasmessi dal Soggetto produttore, memorizzati e conservati nel Sistema di Conservazione e distribuiti ai soggetti abilitati sotto forma di pacchetti informativi. Il *pacchetto informativo*, a seconda sia utilizzato per versare, conservare o distribuire gli oggetti sottoposti a conservazione, assume la forma, rispettivamente, di *Pacchetto di Versamento* (SIP), *Pacchetto di Archiviazione* (AIP) e *Pacchetto di Distribuzione* (DIP).

### 5.5.1 Pacchetto di versamento (SIP)

I SIP sono concordati per struttura e contenuto tra il Produttore ed il Conservatore e contengono l'oggetto o gli oggetti da conservare. In base alle specifiche esigenze possono contenere una o più unità archivistiche, una o più unità documentarie, eventuali aggiornamenti all'unità documentaria già versata o solo informazioni da associare a un'unità documentaria già conservata. Ogni SIP può generare uno o più Pacchetti di Archiviazione così come più SIP possono costituire un unico Pacchetto di Archiviazione.
Per ulteriori dettagli si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici che integrano il presente documento.

### 5.5.2 Pacchetto di archiviazione (AIP)

Il Pacchetto di Archiviazione viene generato dal Sistema di Conservazione in seguito alla conclusione del processo di acquisizione e presa in carico dei SIP. È composto dagli oggetti-dati (file) e dall'*indice dell'AIP*, un file XML che contiene tutti gli elementi del pacchetto informativo, derivati sia dalle informazioni contenute nel SIP (o nei SIP) trasmessi dal Produttore, sia da quelle generate dal Sistema nel corso del Processo di Conservazione.
Per ulteriori dettagli si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici che integrano il presente documento.

### 5.5.3 Pacchetto di distribuzione (DIP)

Il Pacchetto di Distribuzione viene generato dal Sistema a partire dai Pacchetti di Archiviazione conservati ed è finalizzato a mettere a disposizione dei richiedenti abilitati, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione.
Per ulteriori dettagli si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici/schede di attivazione che integrano il presente documento.

# 6 PROCESSO DI CONSERVAZIONE

## 6.1 FASI DEL VERSAMENTO E LOGICHE DI CONSERVAZIONE

Il Processo di Conservazione è attivato come già descritto nel paragrafo 2.
Le procedure per l'attivazione del Processo di Conservazione sono dettagliate in appositi Disciplinari tecnici e Schede di attivazione.
Il Processo di Conservazione si basa su di una logica caratterizzata dal versamento da parte del Produttore degli oggetti da conservare (documenti informatici e aggregazioni documentali informatiche) con le modalità e le procedure descritte nei loro aspetti generali nel manuale di conservazione dei Conservatori e, per gli

aspetti operativi e specifici, nei richiamati Disciplinari tecnici /Schede di attivazione.

## 6.2 ACQUISIZIONE E PRESA IN CARICO DEI PACCHETTI DI VERSAMENTO (SIP)

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici/Schede di attivazione che integrano il presente documento.

### 6.2.1 Pre-acquisizione

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

### 6.2.2 Acquisizione

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

### 6.2.3 Verifica

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

### 6.2.4 Rifiuto o accettazione

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

### 6.2.5 Presa in carico e generazione del Rapporto di versamento

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

### 6.2.6 Generazione del Pacchetto di archiviazione (AIP)

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

## 6.3 GESTIONE DEL PACCHETTO DI ARCHIVIAZIONE (AIP)

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

### 6.3.1 Aggiornamento dei pacchetti di archiviazione (AIP)

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

### 6.3.2 Selezione e scarto dei pacchetti di archiviazione (AIP)

Nel rispetto di quanto stabilito nel piano di conservazione del Soggetto produttore e sulla base di quanto

specificato nei Disciplinari tecnici e Schede di attivazione, i pacchetti di archiviazione, in funzione della tipologia degli oggetti documentali interessati, saranno sottoposti o meno a procedura di scarto coerentemente con eventuali aggiuntive indicazioni da parte del MiBAC.
Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

## 6.4 GESTIONE DEL PACCHETTO DI DISTRIBUZIONE (DIP)

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

### 6.4.1 Modalità di esibizione / estensione

La distribuzione dei pacchetti a fine di esibizione avviene utilizzando gli strumenti messi a disposizione dal Servizio di Conservazione, secondo modalità condivise tra il Responsabile della protezione dati e il Titolare del trattamento dei dati personali.
Inoltre, per quanto specificato in § 3, al personale abilitato del Soggetto produttore è consentita la consultazione di quanto versato in conservazione accedendo alle funzionalità e agli strumenti erogati dal Sistema di Conservazione secondo le modalità e regole fornite dai Conservatori.

Il Soggetto produttore consente l'accesso ai documenti disciplinato dalla l. 241/90 e l'accesso civico ai documenti (ai sensi dell'art. 5, commi 1 e 2, del D. Lgs. 33/2013) disciplinando le relative procedure come riportate nella sezione del portale istituzionale raggiungibile al seguente link Consiglio Regionale del Lazio - urp (regione.lazio.it)

I responsabili dei procedimenti individuati nelle procedure di cui al precedente capoverso, se opportunamente abilitati alla consultazione dei documenti informatici versati in conservazione, ne potranno prendere visione o potranno recuperarli.
Nel caso in cui i predetti responsabili non siano in alcun modo in grado di acquisire i documenti di interesse, gli stessi potranno rivolgere al Responsabile della Conservazione formale richiesta di presa visione e di eventuale recupero dei documenti informatici in conservazione. Il Responsabile della Conservazione, valutati gli elementi che consentono l'individuazione dei documenti, l'identità del richiedente e la sua titolarità all'accesso ai documenti, avvalendosi eventualmente della consulenza del Responsabile della protezione dei dati, si attiva per la ricerca dei documenti richiesti all'interno del Sistema di Conservazione e, in caso di esito favorevole della predetta ricerca, riscontra positivamente la richiesta. Di intesa con il Responsabile della protezione dati e il Titolare del trattamento dei dati personali, è cura del richiedente gestire eventuali dati particolari nelle forme previste dal Codice in materia di protezione dei dati personali (vedasi D. Lgs. 196/2003) e dal Regolamento UE n. 2016/679 relativo alla protezione dei dati personali (GDPR).

### 6.4.2 Produzione di copie e di duplicati

Il Sistema di Conservazione consente il rilascio, al personale opportunamente autorizzato dal Soggetto produttore, di duplicati e copie informatiche dei documenti digitali presenti nei propri archivi, secondo modalità condivise tra il Responsabile della protezione dei dati e il Titolare del trattamento dei dati personali.
La figura del pubblico ufficiale è prevista nel caso in cui sia necessaria la copia conforme di un documento ai sensi delle Linee Guida AgID sul documento informatico.

Per ulteriori dettagli, si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

### 6.4.3 Interoperabilità

Gli accordi di collaborazione tra Soggetto produttore e Conservatori prevedono, alla loro scadenza, nell'ipotesi di recesso di una delle Parti ovvero al termine, per qualsivoglia causa, di validità dello stesso, la restituzione degli oggetti trasferiti e conservati.
Questi ultimi si intendono comprensivi dei metadati e delle evidenze informatiche che comprovano la corretta conservazione degli stessi, fornendo gli elementi necessari per valutarne l'autenticità e la validità giuridica.
I Conservatori provvederanno solo al termine del riversamento all'eliminazione di tutti gli oggetti riversati e di tutti gli elementi riferiti al Soggetto produttore, garantendo la completa cancellazione e non leggibilità dei dati.
L'intera operazione dovrà avvenire con l'autorizzazione e la vigilanza delle competenti autorità, in particolare delle strutture del MiBAC, e del Responsabile della protezione dei dati.
Il Soggetto produttore ha inoltre la possibilità di richiedere ai Conservatori l'acquisizione di documenti informatici e aggregazioni documentali informatiche precedentemente conservate presso altri conservatori o presso il Soggetto produttore.
Per ulteriori dettagli, si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione che integrano il presente documento.

## 6.5 MONITORAGGIO E RISOLUZIONE DELLE ANOMALIE

La segnalazione di un'anomalia o di un incidente può provenire sia dal Soggetto produttore sia dal gestore del Servizio di Conservazione.
Il processo di monitoraggio e gestione delle anomalie si applica a tutti gli incidenti e problemi attinenti alle seguenti aree:

- Anomalia sistemi.
- Anomalia linee di comunicazione.
- Sicurezza informatica.
- Sicurezza fisica/ambientale.
- Anomalia software.
- Problema hardware.

Si rimanda al manuale di conservazione dei Conservatori e ai Disciplinari tecnici e Schede di attivazione, in cui sono definite le specifiche operative e le modalità di interazione per la gestione delle anomalie e per il monitoraggio.

# 7 DESCRIZIONE DEL SISTEMA DI CONSERVAZIONE

## 7.1 COMPONENTI LOGICHE

Si rimanda al manuale di conservazione dei Conservatori.

## 7.2 COMPONENTI FISICHE

Si rimanda al manuale di conservazione dei Conservatori.

### 7.2.1 Schema generale

Si rimanda al manuale di conservazione dei Conservatori.

### 7.2.2 Caratteristiche tecniche del Sito primario

Si rimanda al manuale di conservazione dei Conservatori.

## 7.3 COMPONENTI TECNOLOGICHE

Si rimanda al manuale di conservazione dei Conservatori.

## 7.4 PROCEDURE DI GESTIONE DEL SISTEMA

Si rimanda al manuale di conservazione dei Conservatori.

## 7.5 EVOLUZIONE DEL SISTEMA

Si rimanda al manuale di conservazione dei Conservatori.

## 7.6 MONITORAGGIO E CONTROLLI

### 7.6.1 Procedure di monitoraggio

Il Responsabile della Conservazione vigila sul funzionamento del Sistema di Conservazione interfacciandosi periodicamente con il Responsabile dello sviluppo e della manutenzione del sistema di conservazione dei Conservatori. Le procedure di monitoraggio del sistema sono dettagliate nel manuale di conservazione dei Conservatori.

### 7.6.2 Funzionalità per la verifica e il mantenimento dell'integrità degli archivi

Il Responsabile della Conservazione vigila sull'integrità degli archivi del Sistema di Conservazione interfacciandosi periodicamente con il Responsabile dello sviluppo e della manutenzione del sistema di conservazione dei Conservatori. Nel manuale di conservazione dei Conservatori sono descritte le procedure operative di verifica dell'integrità degli archivi.

### 7.6.3 Casistica e soluzioni adottate in caso di anomalie

Si rimanda al manuale di conservazione dei Conservatori.

# 8 STRATEGIE ADOTTATE A GARANZIA DELLA CONSERVAZIONE

## 8.1 MISURE A GARANZIA DELLA INTELLEGIBILITÀ, DELLA LEGGIBILITÀ E DELLA REPERIBILITÀ NEL TEMPO

Il Responsabile della Conservazione effettua una verifica periodica dell'effettiva disponibilità dei documenti conservati mediante le funzioni messe a disposizione dai Conservatori. Per quanto riguarda i dettagli, si rimanda al manuale di conservazione dei Conservatori.

### 8.2 MISURE A GARANZIA DELL'INTEROPERABILITÀ E DELLA TRASFERIBILITÀ AD ALTRI CONSERVATORI

Il Responsabile della Conservazione vigila sulle misure adottate a garanzia dell'interoperabilità e della trasferibilità ad altri conservatori del Sistema di Conservazione interfacciandosi periodicamente con il Responsabile dello sviluppo e della manutenzione del sistema di conservazione dei Conservatori. Per quanto riguarda i dettagli, si rimanda al manuale di conservazione dei Conservatori.

## 9 TRATTAMENTO DEI DATI PERSONALI

Il Titolare del trattamento ha il compito di tutela delle informazioni contenute nei documenti da conservare; tale compito viene svolto sia dal Titolare stesso, in quanto Soggetto produttore, sia dai Conservatori, nelle forme previste dal Codice in materia di protezione dei dati personali (vedasi Decreto legislativo 30 giugno 2003, n. 196) e dal Regolamento UE n. 2016/679 relativo alla protezione dei dati personali (GDPR).

Con riferimento alle istruzioni cui deve attenersi il personale autorizzato al trattamento dei dati da parte del Titolare, per le diverse tipologie di documenti che verranno inviate in conservazione, si rimanda al Regolamento di organizzazione del Consiglio regionale del Lazio, fermo restando che il trattamento dei dati personali avverrà comunque nel pieno rispetto di quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 e dal Regolamento (UE) 2016/679.

Il Soggetto produttore ha affidato ai Conservatori, dotati di specifica competenza ed esperienza, lo svolgimento del Processo di Conservazione secondo quanto stabilito nell'Accordo siglato con ParER e nel contratto stipulato con InfoCert. Il Soggetto produttore, Titolare dei dati, ha nominato entrambi i Conservatori quale Responsabile (esterno) del trattamento dei dati personali necessari all'esecuzione dei già menzionati accordi e al compimento degli atti conseguenti.

Le attività di trattamento dei dati personali sono svolte nei limiti strettamente necessari alla realizzazione delle prestazioni richieste, unicamente tramite soggetti debitamente autorizzati, secondo i principi previsti dall'art. 5 del Regolamento (UE) 2016/679.

## 10 ALLEGATI

Allegato n. 1 *Disciplinare tecnico ParER*
Allegato n. 2 *Disciplinare tecnico InfoCert*
Allegato n. 3 *Scheda di attivazione InfoCert*

# DISCIPLINARE TECNICO

## PER LO SVOLGIMENTO DELLA FUNZIONE DI CONSERVAZIONE DEI DOCUMENTI INFORMATICI

*Versione del 09/11/2021 (ora:09:42:41)*

Ente convenzionato

*Estremi dell'Accordo/Convenzione tra Ente e Regione Emilia-Romagna per lo svolgimento della funzione di conservazione dei documenti informatici:*

*Data di decorrenza:*
*30/09/2021*
*Data di fine validità:*
*30/09/2026*

Nome dell'Ente versante configurato nel Sistema di conservazione: regione lazio
Descrizione dell'Ente versante:
Regione Lazio

Nome della Struttura versante configurata nel Sistema di conservazione: r_lazio_crl
Descrizione della Struttura versante:
Struttura di test per la Regione Lazio relativa alla documentazione prodotta dal Consiglio Regionale

Soggetto conservatore
**Regione Emilia-Romagna Servizio Polo Archivistico dell'Emilia-Romagna (ParER)**

# INTRODUZIONE

## Scopo, ambito e struttura del documento

Il presente documento costituisce il Disciplinare Tecnico (d'ora in poi Disciplinare), cioè il documento che definisce le specifiche operative e le modalità di descrizione e di versamento nel Sistema di conservazione delle Tipologie di unità documentarie oggetto di conservazione. Il Disciplinare è redatto in esecuzione di quanto indicato nell'Accordo o Convenzione, che regola nei suoi profili generali il rapporto tra l'Ente e Regione Emilia-Romagna per lo svolgimento della funzione di conservazione dei documenti informatici affidati dall'Ente alla Regione Emilia-Romagna e più specificatamente al suo Servizio Polo archivistico dell'Emilia-Romagna (d'ora in poi ParER) in base al Manuale di conservazione (d'ora in poi Manuale) redatto da ParER.
Per lo svolgimento delle funzioni di conservazione dei documenti informatici, ParER ha sviluppato un proprio Sistema di conservazione (d'ora in poi Sistema), descritto nel Manuale.
Le modalità generali di gestione delle funzioni di conservazione sono descritte nel Manuale a cui si rimanda anche per la terminologia utilizzata nel presente Disciplinare.
Il Disciplinare definisce l'articolazione in Strutture (corrispondenti normalmente alle Aree Organizzative Omogenee, ma non escludendo altre ripartizioni) con cui l'Ente si rapporta con ParER per il versamento dei documenti.
Inoltre dettaglia tutti gli aspetti direttamente desumibili dalle configurazioni della struttura versante (d'ora in poi Struttura) nel Sistema e non espressamente trattati dal Manuale. In particolare descrive le specificità e le modalità di versamento dei documenti informatici proprie dell'Ente.
Gli utenti espressamente autorizzati dall'Ente possono accedere al Sistema tramite credenziali personali rilasciate da ParER e comunicate al singolo utente. L'accesso al Sistema consente di consultare i documenti digitali versati nel Sistema e le configurazioni specifiche adottate.

ParER nell'erogazione dei servizi di conservazione garantisce ai Produttori i livelli di servizio che sono riportati nel catalogo dei servizi SaaS pubblicato da AgID alla pagina https://cloud.italia.it/marketplace/show/all?searchCategory=SaaS, in quanto dal 3/3/2020 ParER è fornitore accreditato di Software as a Service nel Cloud delle pubbliche amministrazioni.

## Referenti

In questo capitolo sono definiti i nominativi e i recapiti dei Referenti ParER che seguono o hanno seguito i test di versamento e l'attività di avvio del servizio di conservazione.

| Nome e cognome | Recapiti | Archivista di riferimento (ParER) / Referente Ente | Note |
|---|---|---|---|
| Laura Aliprandi | laura.aliprandi@regione.emilia-romagna.it | Archivista di riferimento (ParER) | |
| Enrico Fagiani | Enrico.fagiani@regione.emilia-romagna.it | Archivista di riferimento (ParER) | |

**Tabella - Referenti**

## Tipologie di unità documentarie

La Tabella Tipologie di unità documentarie elenca le tipologie di unità documentarie oggetto di versamento e restituisce per ciascuna l'informazione relativa al sistema versante e alla data di primo versamento.

Per unità documentaria si intende un aggregato logico costituito da uno più documenti che sono considerati come un tutto unico. I documenti sono gli elementi dell'unità documentaria e sono identificati in base alla funzione che svolgono nel contesto dell'unità documentaria stessa, ovvero:

- Documento principale: documento che deve essere obbligatoriamente presente nell'unità documentaria, della quale definisce il contenuto primario;
- Allegato: documento che compone l'unità documentaria per integrare le informazioni contenute nel documento principale. È redatto contestualmente o precedentemente al documento principale;
- Annesso: documento che compone l'unità documentaria, generalmente prodotto e inserito nell'unità documentaria in un momento successivo a quello di creazione dell'unità documentaria, per fornire ulteriori notizie e informazioni a corredo del documento principale;
- Annotazione: documento che compone l'unità documentaria riportante gli elementi identificativi del documento e del suo iter documentale (un tipico esempio di Annotazione è rappresentato dalla segnatura di protocollo);

Per sistema versante si intende il sistema che cura, sotto forma di pacchetto di versamento (SIP), la trasmissione dei documenti al Sistema, direttamente o tramite sistemi intermedi, esterni all'Ente. Al sistema versante è associato l'utente versatore indicato nel SIP. In caso di utilizzo del client on line di versamento messo a disposizione da ParER o del servizio di versamento asincrono, la colonna Sistema versante sarà compilata rispettivamente con "SACER_VERSO" e "SACER_PREINGEST". Si precisa che il sistema versante e la modalità di versamento possono variare nel tempo e che il versamento della stessa tipologia di unità documentaria può essere

contestualmente curato da più sistemi. In tali casi la tabella riporterà l'indicazione di tutti i sistemi versanti e utenti versatori utilizzati per il versamento.
Nel caso in cui alla data di estrazione del Disciplinare non siano ancora stati effettuati versamenti risolti, le informazioni relative al nome del sistema versante, utente versatore e data di primo versamento non sono riportate nella Tabella Tipologie di unità documentarie.

| Tipologia di unità documentaria | Sistema versante | Utente versatore | Data di primo versamento |
|---|---|---|---|
| DETERMINAZIONE | | | |

**Tabella - Tipologie di unità documentarie**

Nei paragrafi seguenti sono descritte in dettaglio le singole tipologie di unità documentarie in termini di struttura e metadati.

## Tipologia di unità documentaria DETERMINAZIONE

**Descrizione della tipologia di unità documentaria:** Atto formale con il quale i Dirigenti e i Responsabili dei Servizi, manifestano e dichiarano la propria volontà nell'esercizio della potestà di gestione finanziaria tecnica ed amministrativa, anche con l'attività di assunzione degli impegni di spesa

**Tipi struttura dell'unità documentaria:** nella Tabella Tipi struttura unità documentaria sono rappresentate le varie strutture che può assumere il tipo di unità documentaria, ovvero la sua articolazione in documento principale ed eventuali allegati, annessi e annotazioni, le informazioni relative alla chiave, ai metadati di profilo e altro ancora.
Per ogni Tipo struttura è indicato il periodo di validità, ovvero per quali annualità delle unità documentarie è valido il tipo struttura e i sistemi versanti utilizzati.

| Denominazione | Descrizione | Periodi di validità | Sistemi versanti |
|---|---|---|---|
| DETERMINAZIONE | | 2021 | SICER (Laziocrea) |

**Tabella - Tipi struttura unità documentaria**

Nei paragrafi successivi sono riportate le informazioni di dettaglio su ogni singolo Tipo struttura dell'unità documentaria

**Tipo struttura DETERMINAZIONE** Nella tabella è riportata l'articolazione dell'unità documentaria in documento principale ed eventuali allegati, annessi e annotazioni.

| Tipo documento | Descrizione |
|---|---|

| | |
|---|---|
| DETERMINAZIONE | Testo dell'atto |

**Tabella - Tipo struttura DETERMINAZIONE_Descrizione tipi documento**

| Tipo documento | Elemento | Obbligatorio | Periodicità di versamento | Note |
|---|---|---|---|---|
| DETERMINAZIONE | PRINCIPALE | Si | | |

**Tabella - Tipo struttura DETERMINAZIONE_Dettaglio tipi documento**

**Chiave identificativa del tipo struttura dell'unità documentaria (Tipo registro - Anno - Numero)**

**Registri** - Nella Tabella Elenco registri è rappresentata la lista dei registri associati all'unità documentaria. Il nome del registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale avviene l'assegnazione dell'identificativo progressivo e univoco. Il parametro "Fiscale" indica che le unità documentarie associate al Registro sono soggette alla conservazione di tipo fiscale, finalizzata alla conservazione a norma dei documenti rilevanti ai fini tributari in conformità con quanto previsto dalla normativa di settore vigente (DM del 17 giugno 2014 del Ministero dell'economia e delle finanze)

| Tipo registro | Descrizione | Periodi di validità | Descrizione formato numero | Fiscale | Data disattivazione |
|---|---|---|---|---|---|
| A | Repertorio annuale delle determine prodotte dal Consiglio Regionale della Regione Lazio | 2021 | Stringa costituita da caratteri alfanumerici | No | |

**Tabella - Elenco registri**

**Anno** - Anno di registrazione della determinazione nel relativo registro

**Numero** - Numero di registrazione nel registro indicato nell'elemento <TipoRegistro>

**Riferimento temporale** - In alternativa una delle seguenti date: - Data di pubblicazione; - Data di esecutività; - Data di registrazione (Data di protocollazione o repertoriazione) Qualora i riferimenti indicati non fossero disponibili si suggerisce l'utilizzo di una

delle seguenti date: - Data di versamento nel sistema di conservazione; - Data di firma ricavate dal DB del sistema software che produce il documento e non dalla busta crittografica della firma. - Data di trasmissione e di ricezione mediante Posta elettronica certificata

**Metadati di profilo del tipo unità documentaria** – Nella Tabella Metadati di profilo dell'unità documentaria sono descritti i metadati "Data" e "Oggetto" associati all'unità documentaria

| **Denominazione** | **Descrizione** |
|---|---|
| Data | Data di registrazione del documento nel registro indicato nell'elemento <TipoRegistro> In alternativa, una delle seguenti date:<br>- data significativa per il soggetto produttore;<br>- data di stampa o di estrazione del documento. Se date diverse riportare l'ultima in ordine cronologico;<br>- data di firma. Se date diverse riportare l'ultima in ordine cronologico |
| Oggetto | Oggetto della determina indicato nell'atto, qualora disponibile. In alternativa, stringa così composta: "Determina n. [numero di registrazione] del [data di registrazione]" |

**Tabella - Metadati di profilo dell'unità documentaria**

**Periodicità di versamento**: Non nota

**Firme**: Digitale

**Metadati specifici associati al tipo unità documentaria** - Nelle Tabelle Metadati specifici dell'unità documentaria è presentato il set di metadati associato all'unità documentaria nelle diverse versioni. La presenza di versioni diverse è legata alle eventuali modifiche/integrazioni/aggiornamenti nel set di metadati specifici o nelle obbligatorietà concordate con l'Ente.

*Versione metadati specifici: 1.0*
*Descrizione versione: Versione concordata con la Società*
*LAZIOcrea Data inizio validità: 06/05/2020 Data fine*
*validità:*

| Denominazione | Descrizione |
|---|---|
| PropostaIdentificativo | Numero della proposta di Determinazione |
| DataProposta | Data della proposta |
| StrutturaProponente | Struttura che propone la Determinazione o di riferimento del dirigente o responsabile titolare della emanazione dell'atto (può essere definita anche in maniera più specifica: Area, Servizio, Unità, ecc.) |
| Firmatario | Firmatario della Determinazione DATO OBBLIGATORIO |
| RuoloFirmatario | Ruolo o qualifica del firmatario della Determinazione (può essere specificato eventuale funzione di delega) DATO OBBLIGATORIO |
| VistoContabile | Esito dell'eventuale parere contabile (in caso di CONTRARIO la determinazione esiste ma non sarà esecutiva) Valori possibili: NON PREVISTO FAVOREVOLE CONTRARIO |
| ResponsabileVistoContabile | Indica il nome del responsabile del servizio finanziario o di ragioneria o equi valente che appone il visto (per determine con impegno di spesa) |
| DataVistoContabile | Data di emissione del visto di regolarità contabile (per determine con impegno di spesa) |
| NoteVistoContabile | Riporta le motivazione di un visto contrario |
| ImpegnoSpesa | Riferimento all'impegno di spesa (per determine con impegno di spesa) |
| DataEsecutivita | Data di esecutività corrispondente alla data di firma della determinazione d a parte del dirigente (per le determinazioni senza impegno di spesa) o alla data di firma del visto contabile (nel caso di determinazione con impegno di spesa) DATO OBBLIGATORIO |
| TipoPubblicazione | Indicazione circa la pubblicazione integrale o parziale della determina ad esempio pubblicazione della delibera senza gli |

| | |
|---|---|
| | eventuali allegati, parte integrante della stessa, in quanto riservati Valori possibili: PARZIALE / INTEGRALE |
| RegistroPubblicazione | Indicazione del registro di pubblicazione |
| NumeroPubblicazione | Indicazione del numero di pubblicazione sul registro di pubblicazione |
| DataInizioPubblicazione | Data di inizio pubblicazione |
| DataFinePubblicazione | Data di fine pubblicazione |
| FunzionarioAttestantePubblicazione | Nome e cognome del soggetto incaricato di dichiarare l'avvenuta pubblicazione dell'atto |
| AmministrazioneTrasparente | Indicazione circa la pubblicazione della determina sul sito "Amministrazione trasparente" ai sensi del D. Lgs 33/2013 |
| TipoPubblicazioneTrasparenza | Pubblicazione integrale della determina sul sito "Amministrazione trasparente" o i soli dati riassuntivi della stessa<br>Valori possibili: INTEGRALE / DATI RIASSUNTIVI |
| RiferimentoNormativo | Indicazione dell'articolo del D.Lgs. 33/2013 che disciplina l'obbligo di pubblicazione della determina o dei dati riassuntivi della stessa |
| ResponsabilePubblicazioneTrasparenza | Nome e cognome del funzionario responsabile della pubblicazione della determina sul sito "Amministrazione trasparente" |
| Annullamento | Indicazione relativa all'eventuale annullamento della determina<br>Può assumere i valori: SI / NO<br>DATO OBBLIGATORIO |
| AnnullamentoAtto | Estremi dell'atto di annullamento della determina |
| AnnullamentoData | Data dell'annullamento |
| AnnullamentoMotivo | Motivo dell'annullamento |
| AnnullamentoSoggetto | Soggetto che ha autorizzato l'annullamento |

| | |
|---|---|
| Originatore | Denominazione dell'Unità o Settore responsabile della produzione del documento |
| Responsabile | Nominativo del responsabile dell'Unità o del Settore che ha prodotto il documento |
| Operatore | Nominativo dell'operatore che ha creato il documento. Può essere valorizzato con la denominazione del sistema in caso di generazione automatica del documento |
| RegistroAltraRegistrazione | Denominazione del registro in cui è avvenuta l'eventuale e ulteriore registrazione del documento |
| AnnoAltraRegistrazione | Anno dell'eventuale ulteriore registrazione associata al documento |
| NumeroAltraRegistrazione | Numero dell'eventuale ulteriore registrazione associata al documento |
| DataAltraRegistrazione | Data dell'eventuale ulteriore registrazione associata al documento |
| TempoConservazione | Valore ricavato dal piano di conservazione o massimario di scarto. In caso di conservazione permanente inserire la stringa "ILLIMITATA". In caso sia definito il tempo di conservazione inserire il numero di anni in formato numerico |
| Consultabilita | Tipologia di dato contenuto nel documento, sia ai sensi della normativa vigente in materia di privacy (Regolamento UE 2016/679) sia in materia di beni culturali (D.Lgs 42/2004) Valori possibili: "DATI PARTICOLARI" "DATI BIOMETRICI" "RISERVATI" "NON RISERVATI" "DATI PERSONALI" "DATI SENSIBILI" "DATI GENETICI" "DATI GIUDIZIARI" "DATI STATO SALUTE" "DATI VITA SESSUALE" "DATI RAPPORTI RISERVATI FAMILIARI" "NON PRECISATO" |
| DenominazioneApplicativo | Denominazione commerciale dell'applicativo che produce il documento |
| VersioneApplicativo | Versione dell'applicativo che produce il documento |
| ProduttoreApplicativo | Denominazione del produttore dell'applicativo che produce il documento |
| Note | Eventuali note ed osservazioni in relazione al documento |

**Tabella - Metadati specifici dell'unità documentaria**

## Parametri di Struttura per le verifiche al versamento

Nella fase di acquisizione del pacchetto di versamento (SIP) il Sistema effettua una serie di verifiche automatiche finalizzate ad individuare eventuali anomalie. In questo capitolo è descritta l'impostazione dell'intera Struttura in relazione ai controlli operati dal Sistema. Si precisa che l'impostazione della struttura interessa tutte le tipologie documentarie configurate. Il sistema consente inoltre di impostare specifici controlli a livello di singola tipologia documentaria. Le eventuali impostazioni definite per la tipologia documentaria sono dettagliate nel capitolo "Parametri sul tipo unità documentaria per le verifiche al versamento".
Per ciascun parametro sono fornite le seguenti informazioni:
-sintetica descrizione;
-indicazione dello stato di attivazione previsto dalla configurazione "standard" definita da ParER;
- indicazione dello stato di attivazione effettivo.
Si precisa che l'eventuale difformità tra lo stato di attivazione definito da ParER e lo stato effettivo dipende da un'esplicita richiesta di modifica del parametro "standard" da parte dell'Ente. Le verifiche automatiche a cui sono sottoposti i SIP nonché i parametri di accettazione sono infatti regolabili a discrezione dell'Ente.

L'esito del versamento è condizionato dai parametri impostati a livello di Struttura dettagliati nelle tabelle sottostanti e dai parametri definiti dall'Ente a livello di Indice SIP (file XML che contiene i metadati nonché i riferimenti ai file dei Componenti del SIP dell'unità documentaria).
I parametri definiti nell'Indice SIP sono tre:
-Forza Accettazione: definisce il comportamento del Sistema in relazione agli esiti delle verifiche di firma e/o formato dei file contenuti nel SIP. Assume valori "False" o "True":
  - False: il Sistema accetta il versamento solo se tutti i controlli relativi alla firma e al formato hanno esito positivo
  - True: il Sistema accetta il versamento anche nel caso in cui almeno uno dei controlli relativi alla firma e al formato hanno esito negativo
-Forza Conservazione: definisce il comportamento del Sistema in relazione al versamento di SIP contenenti file non firmati. Assume valori "False" o "True":
  - False: il Sistema accetta il versamento solo se e` presente almeno un file firmato
  - True: il Sistema accetta il versamento anche nel caso in cui nessuno dei file sia firmato
-Forza Collegamento: definisce il comportamento del Sistema in funzione della presenza o meno nel Sistema stesso del SIP oggetto di collegamento. Assume valori "False" o "True":
  - False: il Sistema accetta il versamento di SIP i cui eventuali Collegamenti siano rivolti a SIP gia` presenti nel Sistema
  - True: il Sistema accetta il versamento di SIP anche nel caso in cui gli eventuali Collegamenti siano rivolti a SIP non presenti nel Sistema.

L'impostazione "standard" riguarda unicamente i parametri configurati a livello di Struttura e prevede l'attivazione di tutti i controlli sul formato del file e sulla validità della firma e di tutti i relativi parametri di accettazione dei SIP per i quali il Sistema abbia restituito un esito negativo del controllo.

Si precisa che i controlli sulle eventuali firme digitali è effettuata alla data indicata nell'Indice SIP (che puo` essere quella contenuta nella firma, in una marca temporale o un riferimento temporale dichiarato nell'Indice SIP) o, in assenza di questa, alla data del versamento.
Secondo l'impostazione "standard", il SIP con esito negativo del controllo sulla validità della firma viene accettato in conservazione solo se la trasmissione dello stesso viene "forzata" dal versatore in sede di versamento. La forzatura consiste nel valorizzare con "True" il parametro "Forza Accettazione" presente nell'Indice SIP.
A titolo di esempio si riporta l'esito del versamento di un SIP con certificato di firma scaduto in relazione all'impostazione del parametro "Forza Accettazione" e all'impostazione "standard" dei parametri di Struttura:

**CASO A** – *Parametro "Forza Accettazione" attivo*
- Controllo certificato: SI (configurazione standard)
- Accetta controllo certificato scaduto: SI (configurazione standard)
- Forza Accettazione: SI (definito nell'Indice SIP)

In questo caso il SIP viene acquisito in conservazione e l'esito del versamento è di tipo WARNING.
**CASO B** – *Parametro "Forza Accettazione" NON attivo*
- Controllo certificato: SI (configurazione standard)
- Accetta controllo certificato scaduto: SI (configurazione standard)
- Forza Accettazione: NO (definito nell'Indice SIP)

In questo caso il SIP viene rifiutato e l'esito del versamento è NEGATIVO.

Il registro viene definito dall'Ente o concordato con ParER e in generale corrisponde al nome del repertorio in cui sono registrati in ordine progressivo i documenti ad esso afferenti (ex art. 53, D.P.R. 28/12/2000 n. 445) oppure al contesto applicativo/documentale nell'ambito del quale viene attribuito all'unità documentaria l'identificativo progressivo e univoco.
In relazione a ciascun registro associato alle tipologie documentarie oggetto di versamento (vedere Tabella Elenco registri), è definito il formato del metadato "Numero" della chiave del SIP dell'unità documentaria afferente al registro medesimo. Il metadato "Numero" può assumere caratteri diversi ad esempio numerici, alfabetici, alfanumerici, caratteri speciali o numeri romani.
Il Sistema verifica che il valore inserito nel metadato "Numero" risponda al formato definito.
In assenza di indicazioni concordate con l'Ente, il numero della chiave viene accettato come se fosse una stringa (calcolo di ordinamento del numero di tipo "GENERICO").

| Funzione | Parametro | Descrizione | Valore standard | Valore effettivo (Richiesto dall'Ente) |
|---|---|---|---|---|
| Abilitazione fascicoli | FL_GEST_FASCICOLI | Abilita la gestione dei fascicoli nella Struttura (false, true) | SI | SI |

| | | | | |
|---|---|---|---|---|
| Accettazione formati file | FL_ABILITA_CONTR_FMT | Abilita il controllo del formato file versato (false, true) | SI | SI |
| Accettazione formati file | FL_ACCETTA_CONTR_FMT_NEG | Consente di superare un esito controllo formato file negativo con il Forza formato (false, true) | SI | SI |
| Accettazione formati file | FL_FORZA_FMT | Forza l'accettazione del controllo formato file negativo (false, true) | SI | SI |
| Accettazione formati numero unità doc | FL_ABILITA_CONTR_FMT_NUM | Abilita il controllo del formato del numero dell'unità doc (false, true) | SI | SI |
| Accettazione formati numero unità doc | FL_ACCETTA_FMT_NUM_NEG | Consente di superare un esito controllo formato del numero dell'unità doc negativo con il Forza formato (false, true) | NO | NO |
| Accettazione formati numero unità doc | FL_FORZA_FMT_NUM | Forza l'accettazione del controllo formato del numero dell'unità doc negativo (false, true) | NO | NO |
| Accettazione hash versato | FL_ABILITA_CONTR_HASH_VERS | Abilita il controllo del hash versato (false, true) | NO | NO |
| Accettazione hash versato | FL_ACCETTA_CONTR_HASH_NEG | Consente di superare un esito controllo hash versato negativo con il Forza hash versato (false, true) | SI | SI |
| Accettazione hash versato | FL_FORZA_HASH_VERS | Forza l'accettazione del controllo hash versato negativo (false, true) | SI | SI |
| Aggiornamento metadati | FL_ABILITA_UPD_META | Indica se e' abilitato il servizio di aggiornamento metadati unita' doc (false, true) | NO | NO |
| Aggiornamento metadati | FL_ACCETTA_UPD_META_INARK | Indica si accetta l'aggiornamento metadati per unita' doc in archivio con il Forza aggiornamento (false, true) | NO | NO |
| Aggiornamento metadati | FL_FORZA_UPD_META_INARK | Indica se si forza l'aggiornamento metadati per unita' doc in archivio (false, true) | NO | NO |

| | | | | |
|---|---|---|---|---|
| Aggiunta documento | FL_ABILITA_FORZA_DOC_AGG | Abilita Forza aggiunta documento(false, true) | SI | SI |
| Aggiunta documento | FL_ACCETTA_DOC_AGG_NEG | Consente di superare un esito di controllo negativo per documento aggiunto(false, true) | NO | NO |
| Aggiunta documento | FL_FORZA_DOC_AGG | Forza l'accettazione del controllo per documento aggiunto negativo (false, true) | NO | NO |
| Controlli file non firmati | FL_ABILITA_CONTR_NON_FIRMATI | Consente di abilitare/disabilitare la conservazione del documento (false, true) | SI | SI |
| Controlli file non firmati | FL_ACCETTA_CONTR_NON_FIRMATI_NEG | Consente di superare un esito documento non firmato digitalmente con il Forza conservazione (false, true) | SI | SI |
| Controlli file non firmati | FL_FORZA_CONTR_NON_FIRMATI_NEG | Forza l'accettazione di conservazione documento non firmato digitalmente (false, true) | NO | NO |
| Controlli firma CRL | FL_ABILITA_CONTR_CRL_VERS | Abilita il controllo sulla revoca del certificato (false, true) | SI | SI |
| Controlli firma CRL | FL_ACCETTA_CONTR_CRL_NEG | Consente di superare un esito di controllo CRL negativo con il Forza accettazione (false, true) | SI | SI |
| Controlli firma CRL | FL_ACCETTA_CONTR_CRL_NOSCAR | Consente di superare un esito di controllo CRL non scaricabile con il Forza accettazione (false, true) | SI | SI |
| Controlli firma CRL | FL_ACCETTA_CONTR_CRL_NOVAL | Consente di superare un esito di controllo CRL non valida con il Forza accettazione (false, true) | SI | SI |
| Controlli firma CRL | FL_ACCETTA_CONTR_CRL_SCAD | Consente di superare un esito di controllo CRL scaduta con il Forza accettazione (false, true) | SI | SI |
| Controlli firma CRL | FL_FORZA_CONTR_CRL_VERS | Forza il superamento del controllo sulla revoca del certificato (false, true) | SI | SI |
| Controlli firma certificato | FL_ABILITA_CONTR_CERTIF_VERS | Abilita il controllo sulla validità del certificato di firma (false, true) | SI | SI |

| | | | | |
|---|---|---|---|---|
| Controlli firma certificato | FL_ACCETTA_CONTR_CERTIF_NOCERT | Consente di superare un esito di controllo certificato che non e' un certificato con il Forza accettazione (false, true) | SI | SI |
| Controlli firma certificato | FL_ACCETTA_CONTR_CERTIF_NOVAL | Consente di superare un esito di controllo certificato non valido con il Forza accettazione (false, true) | SI | SI |
| Controlli firma certificato | FL_ACCETTA_CONTR_CERTIF_SCAD | Consente di superare un esito di controllo certificato scaduto con il Forza accettazione (false, true) | SI | SI |
| Controlli firma certificato | FL_FORZA_CONTR_CERTIF_VERS | Forza il superamento del controllo sulla validità del certificato di firma (false, true) | SI | SI |
| Controlli firma crittografico | FL_ABILITA_CONTR_CRITTOG_VERS | Abilita il controllo crittografico (false, true) | SI | SI |
| Controlli firma crittografico | FL_ACCETTA_CONTR_CRITTOG_NEG | Consente di superare un esito di controllo crittografico negativo con il Forza accettazione (false, true) | SI | SI |
| Controlli firma crittografico | FL_FORZA_CONTR_CRITTOG_VERS | Forza il superamento del controllo crittografico (false, true) | SI | SI |
| Controlli firma non conforme | FL_ABILITA_VERIFICA_FIRMA | Consente di abilitare/disabilitare i servizi di verifica firma, prima EIDAS, eventualmente CRYPTO (false, true). Nota : se FL_ABILITA_VERIFICA_FIRMA_SOLO_CRYPTO e FL_ABILITA_VERIFICA_FIRMA entrambi false non si effettua la verifica firma | SI | SI |
| Controlli firma non conforme | FL_ACCETTA_FIRMA_GIUGNO_2011 | Consente di superare un esito di controllo negativo per firma no delibera 45 con il Forza accettazione (false, true) | SI | SI |

| | | | | |
|---|---|---|---|---|
| Controlli firma non conforme | FL_ACCETTA_FIRMA_NOCONF | Consente di superare un esito di controllo negativo per firma non conforme con il Forza accettazione (false, true) | SI | SI |
| Controlli firma non conforme | FL_ACCETTA_FIRMA_NOCONOS | Consente di superare un esito di controllo negativo per firma sconosciuta con il Forza accettazione (false, true) | SI | SI |
| Controlli firma non conforme | FL_ACCETTA_MARCA_NOCONOS | Consente di superare un esito di controllo negativo per marca sconosciuta con il Forza accettazione (false, true) | SI | SI |
| Controlli firma non conforme | FL_FORZA_CONTR_NOCONF | Forza il superamento del controllo di conformità (false, true) | SI | SI |
| Controlli firma trusted | FL_ABILITA_CONTR_TRUST_VERS | Abilita il controllo di catena trusted (false, true) | SI | SI |
| Controlli firma trusted | FL_ACCETTA_CONTR_TRUST_NEG | Consente di superare un esito di controllo catena trusted negativo con il Forza accettazione (false, true) | SI | SI |
| Controlli firma trusted | FL_FORZA_CONTR_TRUST_VERS | Forza il superamento del controllo di catena trusted (false, true) | SI | SI |
| Controllo classificazione | FL_ABILITA_CONTR_CLASSIF | Abilita il controllo della classificazione dei fascicoli (false, true) | NO | NO |
| Controllo classificazione | FL_ACCETTA_CONTR_CLASSIF_NEG | Consente di superare un esito del controllo della classificazione negativo con il Forza controllo classificazione (false, true) | NO | NO |
| Controllo classificazione | FL_FORZA_CONTR_CLASSIF | Forza l'accettazione del controllo classificazione negativo (false, true) | NO | NO |
| Controllo collegamenti fascicoli | FL_ABILITA_CONTR_COLLEG | Abilita il controllo dei collegamenti fra fascicoli (false, true) | NO | NO |

| | | | | |
|---|---|---|---|---|
| Controllo collegamenti fascicoli | FL_ACCETTA_CONTR_COLLEG_NEG_FAS | Consente di superare un esito del controllo collegamenti fra fascicoli negativo con il Forza controllo collegamenti (false, true) | SI | SI |
| Controllo collegamenti fascicoli | FL_FORZA_CONTR_COLLEG | Forza l'accettazione del controllo collegamenti fra fascicoli negativo (false, true) | NO | NO |
| Controllo collegamenti fra unità doc | FL_ABILITA_CONTR_COLLEG_UD | Abilita il controllo dei collegameti fra unità doc (false, true) | SI | SI |
| Controllo collegamenti fra unità doc | FL_ACCETTA_CONTR_COLLEG_NEG | Consente di superare un esito controllo collegamenti negativo con il Forza collegamenti (false, true) | NO | NO |
| Controllo collegamenti fra unità doc | FL_FORZA_COLLEG | Forza l'accettazione del controllo collegamenti negativo (false, true) | NO | NO |
| Controllo formato numero fascicoli | FL_ABILITA_CONTR_NUMERO | Abilita il controllo del numero dei fascicoli (false, true) | NO | NO |
| Controllo formato numero fascicoli | FL_ACCETTA_CONTR_NUMERO_NEG | Consente di superare un esito del controllo numero fascicolo negativo con il Forza controllo numero (false, true) | NO | NO |
| Controllo formato numero fascicoli | FL_FORZA_CONTR_NUMERO | Forza l'accettazione del controllo numero fascicolo negativo (false, true) | NO | NO |
| Obbligatorietà dati di profilo unita' doc | FL_OBBL_DATA | Indica se la data e' obbligatoria al versamento (false, true) | SI | SI |

| | | | | |
|---|---|---|---|---|
| Obbligatorietà dati di profilo unita' doc | FL_OBBL_OGGETTO | Indica se l'oggetto e' obbligatorio al versamento (false, true) | SI | SI |

## Formati ammessi

Nella Tabella Formati sono elencati i formati configurati nella struttura. In base all'impostazione "standard" tutti i formati classificati come IDONEI e GESTITI ai fini della conservazione a lungo termini sono inclusi nella struttura mentre i formati classificati come DEPRECATI possono essere ammessi solo su richiesta dell'Ente.

In base all'idoneità in relazione alla conservazione a lungo termine i formati sono classificati come segue:

- Formati idonei: sono i formati che per le loro caratteristiche di standardizzazione, di apertura, di sicurezza, di portabilità, di immodificabilità, di staticità e di diffusione reputati idonei alla conservazione a lungo termine, quali ad esempio quelli elencati al punto 5 dell'Allegato 2 alle Regole tecniche;
- Formati gestiti: sono i formati non ritenuti idonei per la conservazione a lungo termine ma che possono essere opportunamente migrati in Formati idonei, con le procedure di cui al comma 1, lettera j, dell'art. 9 delle Regole tecniche per la produzione delle Copie informatiche di documento informatico;
- Formati deprecati: sono formati ritenuti non idonei per la conservazione a lungo termine e che al contempo non possono essere migrati in Formati idonei, per i quali, quindi, non è possibile assicurare la conservazione a lungo termine.

| **Formato versato ammesso** | **Mimetype** | **Idoneità alla conservazione** |
|---|---|---|
| 7Z | application/x-7z-compressed | GESTITO |
| 7Z.ASICE | application/x-7z-compressed | GESTITO |
| 7Z.ASICS | application/x-7z-compressed | GESTITO |
| 7Z.P7M | application/x-7z-compressed | GESTITO |
| 7Z.P7S | application/x-7z-compressed | GESTITO |
| ACE | application/x-ace-compressed | IDONEO |

| | | |
|---|---|---|
| ACE.ASICE | application/x-ace-compressed | IDONEO |
| ACE.ASICS | application/x-ace-compressed | IDONEO |
| ACE.P7M | application/x-ace-compressed | IDONEO |
| ACE.P7S | application/x-ace-compressed | IDONEO |
| ASF | video/x-ms-asf | GESTITO |
| ASICE | application/vnd.etsi.asic-e+zip | GESTITO |
| ASICS | application/vnd.etsi.asic-s+zip | GESTITO |
| AXX | application/octet-stream | GESTITO |
| AXX.ASICE | application/octet-stream | GESTITO |
| AXX.ASICS | application/octet-stream | GESTITO |
| AXX.P7M | application/octet-stream | GESTITO |
| AXX.P7S | application/octet-stream | GESTITO |
| BMP | image/x-ms-bmp | IDONEO |
| BMP.ASICE | image/x-ms-bmp | IDONEO |
| BMP.ASICS | image/x-ms-bmp | IDONEO |
| BMP.P7M | image/x-ms-bmp | IDONEO |
| BMP.P7S | image/x-ms-bmp | IDONEO |
| CER | application/octet-stream | GESTITO |
| CER.ASICE | application/octet-stream | GESTITO |

| | | |
|---|---|---|
| CER.ASICS | application/octet-stream | GESTITO |
| CER.P7M | application/octet-stream | GESTITO |
| CER.P7S | application/octet-stream | GESTITO |
| CPG | text/plain | GESTITO |
| CPG.ASICE | text/plain | GESTITO |
| CPG.ASICS | text/plain | GESTITO |
| CPG.P7M | text/plain | GESTITO |
| CPG.P7S | text/plain | GESTITO |
| CRL | application/octet-stream | GESTITO |
| CRL.ASICE | application/octet-stream | GESTITO |
| CRL.ASICS | application/octet-stream | GESTITO |
| CRL.P7M | application/octet-stream | GESTITO |
| CRL.P7S | application/octet-stream | GESTITO |
| CSS | text/plain | IDONEO |
| CSS.ASICE | text/plain | IDONEO |
| CSS.ASICS | text/plain | IDONEO |
| CSS.P7M | text/plain | IDONEO |
| CSS.P7S | text/plain | IDONEO |
| CSV | text/plain | IDONEO |

| | | |
|---|---|---|
| CSV.ASICE | text/plain | IDONEO |
| CSV.ASICS | text/plain | IDONEO |
| CSV.P7M | text/plain | IDONEO |
| CSV.P7S | text/plain | IDONEO |
| DBF | application/x-dbf | GESTITO |
| DBF.ASICE | application/x-dbf | GESTITO |
| DBF.ASICS | application/x-dbf | GESTITO |
| DBF.P7M | application/x-dbf | GESTITO |
| DBF.P7S | application/x-dbf | GESTITO |
| DER | application/x-x509-ca-cert | GESTITO |
| DER.ASICE | application/x-x509-ca-cert | GESTITO |
| DER.ASICS | application/x-x509-ca-cert | GESTITO |
| DER.P7M | application/x-x509-ca-cert | GESTITO |
| DER.P7S | application/x-x509-ca-cert | GESTITO |
| DIB | image/x-ms-bmp | IDONEO |
| DIB.ASICE | image/x-ms-bmp | IDONEO |
| DIB.ASICS | image/x-ms-bmp | IDONEO |
| DIB.P7M | image/x-ms-bmp | IDONEO |
| DIB.P7S | image/x-ms-bmp | IDONEO |

| | | |
|---|---|---|
| DOC | application/msword | GESTITO |
| DOC.ASICE | application/msword | GESTITO |
| DOC.ASICS | application/msword | GESTITO |
| DOC.P7M | application/msword | GESTITO |
| DOC.P7S | application/msword | GESTITO |
| DOCX | application/vnd.openxmlformatsofficedocument.wordprocessingml.document | GESTITO |
| DOCX.ASICE | application/vnd.openxmlformatsofficedocument.wordprocessingml.document | GESTITO |
| DOCX.ASICS | application/vnd.openxmlformatsofficedocument.wordprocessingml.document | GESTITO |
| DOCX.P7M | application/vnd.openxmlformatsofficedocument.wordprocessingml.document | GESTITO |
| DOCX.P7S | application/vnd.openxmlformatsofficedocument.wordprocessingml.document | GESTITO |
| DOT | application/msword | GESTITO |
| DOT.ASICE | application/msword | GESTITO |
| DOT.ASICS | application/msword | GESTITO |
| DOT.P7M | application/msword | GESTITO |
| DOT.P7S | application/msword | GESTITO |
| DOTX | application/vnd.openxmlformatsofficedocument.wordprocessingml.template | GESTITO |

| | | |
|---|---|---|
| DOTX.ASICE | application/vnd.openxmlformatsofficedocument.wordprocessingml.template | GESTITO |
| DOTX.ASICS | application/vnd.openxmlformatsofficedocument.wordprocessingml.template | GESTITO |
| DOTX.P7M | application/vnd.openxmlformatsofficedocument.wordprocessingml.template | GESTITO |
| DOTX.P7S | application/vnd.openxmlformatsofficedocument.wordprocessingml.template | GESTITO |
| DTD | text/plain | IDONEO |
| DTD.ASICE | text/plain | IDONEO |
| DTD.ASICS | text/plain | IDONEO |
| DTD.P7M | text/plain | IDONEO |
| DTD.P7S | text/plain | IDONEO |
| DWF | model/vnd.dwf | GESTITO |
| DWF.ASICE | model/vnd.dwf | GESTITO |
| DWF.ASICS | model/vnd.dwf | GESTITO |
| DWF.P7M | model/vnd.dwf | GESTITO |
| DWF.P7S | model/vnd.dwf | GESTITO |
| DWFX | model/vnd.dwfx+xps | GESTITO |
| DWFX.ASICE | model/vnd.dwfx+xps | GESTITO |
| DWFX.ASICS | model/vnd.dwfx+xps | GESTITO |

| | | |
|---|---|---|
| DWFX.P7M | model/vnd.dwfx+xps | GESTITO |
| DWFX.P7S | model/vnd.dwfx+xps | GESTITO |
| DXF | image/vnd.dxf | GESTITO |
| DXF.ASICE | image/vnd.dxf | GESTITO |
| DXF.ASICS | image/vnd.dxf | GESTITO |
| DXF.P7M | image/vnd.dxf | GESTITO |
| DXF.P7S | image/vnd.dxf | GESTITO |
| EML | message/rfc822 | IDONEO |
| EML.ASICE | message/rfc822 | IDONEO |
| EML.ASICS | message/rfc822 | IDONEO |
| EML.P7M | message/rfc822 | IDONEO |
| EML.P7S | message/rfc822 | IDONEO |
| EMLX | message/x-emlx | GESTITO |
| EMLX.ASICE | message/x-emlx | GESTITO |
| EMLX.ASICS | message/x-emlx | GESTITO |
| EMLX.P7M | message/x-emlx | GESTITO |
| EMLX.P7S | message/x-emlx | GESTITO |
| EPS | application/postscript | GESTITO |
| EPS.ASICE | application/postscript | GESTITO |

| | | |
|---|---|---|
| EPS.ASICS | application/postscript | GESTITO |
| EPS.P7M | application/postscript | GESTITO |
| EPS.P7S | application/postscript | GESTITO |
| FO | application/xslfo+xml | IDONEO |
| FO.ASICE | application/xslfo+xml | IDONEO |
| FO.ASICS | application/xslfo+xml | IDONEO |
| FO.P7M | application/xslfo+xml | IDONEO |
| FO.P7S | application/xslfo+xml | IDONEO |
| FODG | application/vnd.oasis.opendocument.graphics-flat-xml | GESTITO |
| FODG.ASICE | application/vnd.oasis.opendocument.graphics-flat-xml | GESTITO |
| FODG.ASICS | application/vnd.oasis.opendocument.graphics-flat-xml | GESTITO |
| FODG.P7M | application/vnd.oasis.opendocument.graphics-flat-xml | GESTITO |
| FODG.P7S | application/vnd.oasis.opendocument.graphics-flat-xml | GESTITO |
| GIF | image/gif | IDONEO |
| GIF.ASICE | image/gif | IDONEO |
| GIF.ASICS | image/gif | IDONEO |
| GIF.P7M | image/gif | IDONEO |
| GIF.P7S | image/gif | IDONEO |

| | | |
|---|---|---|
| GZ | application/gzip | GESTITO |
| GZ.ASICE | application/gzip | GESTITO |
| GZ.ASICS | application/gzip | GESTITO |
| GZ.P7M | application/gzip | GESTITO |
| GZ.P7S | application/gzip | GESTITO |
| HTM | text/html | GESTITO |
| HTM.ASICE | text/html | GESTITO |
| HTM.ASICS | text/html | GESTITO |
| HTM.P7M | text/html | GESTITO |
| HTM.P7S | text/html | GESTITO |
| HTML | text/html | GESTITO |
| HTML.ASICE | text/html | GESTITO |
| HTML.ASICS | text/html | GESTITO |
| HTML.P7M | text/html | GESTITO |
| HTML.P7S | text/html | GESTITO |
| ICO | image/vnd.microsoft.icon | IDONEO |
| ICO.ASICE | image/vnd.microsoft.icon | IDONEO |
| ICO.ASICS | image/vnd.microsoft.icon | IDONEO |
| ICO.P7M | image/vnd.microsoft.icon | IDONEO |

| | | |
|---|---|---|
| ICO.P7S | image/vnd.microsoft.icon | IDONEO |
| INDD | application/x-adobe-indesign | GESTITO |
| INDD.ASICE | application/x-adobe-indesign | GESTITO |
| INDD.ASICS | application/x-adobe-indesign | GESTITO |
| INDD.P7M | application/x-adobe-indesign | GESTITO |
| INDD.P7S | application/x-adobe-indesign | GESTITO |
| JFIF | image/jpeg | IDONEO |
| JFIF.ASICE | image/jpeg | IDONEO |
| JFIF.ASICS | image/jpeg | IDONEO |
| JFIF.P7M | image/jpeg | IDONEO |
| JFIF.P7S | image/jpeg | IDONEO |
| JP2 | image/jp2 | GESTITO |
| JP2.ASICE | image/jp2 | GESTITO |
| JP2.ASICS | image/jp2 | GESTITO |
| JP2.P7M | image/jp2 | GESTITO |
| JP2.P7S | image/jp2 | GESTITO |
| JPE | image/jpeg | IDONEO |
| JPE.ASICE | image/jpeg | IDONEO |
| JPE.ASICS | image/jpeg | IDONEO |

| | | |
|---|---|---|
| JPE.P7M | image/jpeg | IDONEO |
| JPE.P7S | image/jpeg | IDONEO |
| JPEG | image/jpeg | IDONEO |
| JPEG.ASICE | image/jpeg | IDONEO |
| JPEG.ASICS | image/jpeg | IDONEO |
| JPEG.P7M | image/jpeg | IDONEO |
| JPEG.P7S | image/jpeg | IDONEO |
| JPG | image/jpeg | IDONEO |
| JPG.ASICE | image/jpeg | IDONEO |
| JPG.ASICS | image/jpeg | IDONEO |
| JPG.P7M | image/jpeg | IDONEO |
| JPG.P7S | image/jpeg | IDONEO |
| JSON | text/plain | GESTITO |
| JSON.ASICE | text/plain | GESTITO |
| JSON.ASICS | text/plain | GESTITO |
| JSON.P7M | text/plain | GESTITO |
| JSON.P7S | text/plain | GESTITO |
| KML | application/vnd.google-earth.kml+xml | GESTITO |
| KML.ASICE | application/vnd.google-earth.kml+xml | GESTITO |

| | | |
|---|---|---|
| KML.ASICS | application/vnd.google-earth.kml+xml | GESTITO |
| KML.P7M | application/vnd.google-earth.kml+xml | GESTITO |
| KML.P7S | application/vnd.google-earth.kml+xml | GESTITO |
| KMZ | application/vnd.google-earth.kmz | GESTITO |
| KMZ.ASICE | application/vnd.google-earth.kmz | GESTITO |
| KMZ.ASICS | application/vnd.google-earth.kmz | GESTITO |
| KMZ.P7M | application/vnd.google-earth.kmz | GESTITO |
| KMZ.P7S | application/vnd.google-earth.kmz | GESTITO |
| LOG | text/plain | GESTITO |
| LOG.ASICE | text/plain | GESTITO |
| LOG.ASICS | text/plain | GESTITO |
| LOG.P7M | text/plain | GESTITO |
| LOG.P7S | text/plain | GESTITO |
| LYR | application/octetstream | GESTITO |
| M7M | multipart/mixed | IDONEO |
| MHT | message/rfc822 | IDONEO |
| MHT.ASICE | message/rfc822 | IDONEO |
| MHT.ASICS | message/rfc822 | IDONEO |
| MHT.P7M | message/rfc822 | IDONEO |

| | | |
|---|---|---|
| MHT.P7S | message/rfc822 | IDONEO |
| MKV | application/x-matroska | GESTITO |
| MOD | audio/x-mod | GESTITO |
| MSG | application/vnd.ms-outlook | GESTITO |
| MSG.ASICE | application/vnd.ms-outlook | GESTITO |
| MSG.ASICS | application/vnd.ms-outlook | GESTITO |
| MSG.P7M | application/vnd.ms-outlook | GESTITO |
| MSG.P7S | application/vnd.ms-outlook | GESTITO |
| ODB | application/vnd.oasis.opendocument.base | GESTITO |
| ODB.ASICE | application/vnd.oasis.opendocument.base | GESTITO |
| ODB.ASICS | application/vnd.oasis.opendocument.base | GESTITO |
| ODB.P7M | application/vnd.oasis.opendocument.base | GESTITO |
| ODB.P7S | application/vnd.oasis.opendocument.base | GESTITO |
| ODF | application/vnd.oasis.opendocument.formula | IDONEO |
| ODF.ASICE | application/vnd.oasis.opendocument.formula | IDONEO |
| ODF.ASICS | application/vnd.oasis.opendocument.formula | IDONEO |
| ODF.P7M | application/vnd.oasis.opendocument.formula | IDONEO |
| ODF.P7S | application/vnd.oasis.opendocument.formula | IDONEO |
| ODG | application/vnd.oasis.opendocument.graphics | GESTITO |

| | | |
|---|---|---|
| ODG.ASICE | application/vnd.oasis.opendocument.graphics | GESTITO |
| ODG.ASICS | application/vnd.oasis.opendocument.graphics | GESTITO |
| ODG.P7M | application/vnd.oasis.opendocument.graphics | GESTITO |
| ODG.P7S | application/vnd.oasis.opendocument.graphics | GESTITO |
| ODP | application/vnd.oasis.opendocument.presentation | GESTITO |
| ODP.ASICE | application/vnd.oasis.opendocument.presentation | GESTITO |
| ODP.ASICS | application/vnd.oasis.opendocument.presentation | GESTITO |
| ODP.P7M | application/vnd.oasis.opendocument.presentation | GESTITO |
| ODP.P7S | application/vnd.oasis.opendocument.presentation | GESTITO |
| ODS | application/vnd.oasis.opendocument.spreadsheet | GESTITO |
| ODS.ASICE | application/vnd.oasis.opendocument.spreadsheet | GESTITO |
| ODS.ASICS | application/vnd.oasis.opendocument.spreadsheet | GESTITO |
| ODS.P7M | application/vnd.oasis.opendocument.spreadsheet | GESTITO |
| ODS.P7S | application/vnd.oasis.opendocument.spreadsheet | GESTITO |
| ODT | application/vnd.oasis.opendocument.text | GESTITO |
| ODT.ASICE | application/vnd.oasis.opendocument.text | GESTITO |
| ODT.ASICS | application/vnd.oasis.opendocument.text | GESTITO |
| ODT.P7M | application/vnd.oasis.opendocument.text | GESTITO |
| ODT.P7S | application/vnd.oasis.opendocument.text | GESTITO |

| | | |
|---|---|---|
| OFT | application/vnd.ms-outlook | GESTITO |
| OFT.ASICE | application/vnd.ms-outlook | GESTITO |
| OFT.ASICS | application/vnd.ms-outlook | GESTITO |
| OFT.P7M | application/vnd.ms-outlook | GESTITO |
| OFT.P7S | application/vnd.ms-outlook | GESTITO |
| OPUS | audio/opus | GESTITO |
| OPUS.ASICE | audio/opus | GESTITO |
| OPUS.ASICS | audio/opus | GESTITO |
| OPUS.P7M | audio/opus | GESTITO |
| OPUS.P7S | audio/opus | GESTITO |
| OTS | application/vnd.oasis.opendocument.spreadsheet-template | GESTITO |
| OTS.ASICE | application/vnd.oasis.opendocument.spreadsheet-template | GESTITO |
| OTS.ASICS | application/vnd.oasis.opendocument.spreadsheet-template | GESTITO |
| OTS.P7M | application/vnd.oasis.opendocument.spreadsheet-template | GESTITO |
| OTS.P7S | application/vnd.oasis.opendocument.spreadsheet-template | GESTITO |
| OTT | application/vnd.oasis.opendocument.text-template | GESTITO |
| OTT.ASICE | application/vnd.oasis.opendocument.text-template | GESTITO |
| OTT.ASICS | application/vnd.oasis.opendocument.text-template | GESTITO |

| | | |
|---|---|---|
| OTT.P7M | application/vnd.oasis.opendocument.text-template | GESTITO |
| OTT.P7S | application/vnd.oasis.opendocument.text-template | GESTITO |
| P7M | application/pkcs7-mime | GESTITO |
| P7S | application/pkcs7-signature | GESTITO |
| P7S.ASICE | application/pkcs7-signature | GESTITO |
| P7S.ASICS | application/pkcs7-signature | GESTITO |
| P7S.P7M | application/pkcs7-signature | GESTITO |
| P7S.P7S | application/pkcs7-signature | GESTITO |
| P7X | multipart/mixed | GESTITO |
| PDF | application/pdf | IDONEO |
| PDF.ASICE | application/pdf | IDONEO |
| PDF.ASICS | application/pdf | IDONEO |
| PDF.P7M | application/pdf | IDONEO |
| PDF.P7S | application/pdf | IDONEO |
| PGM | image/x-portable-graymap | GESTITO |
| PNG | image/png | GESTITO |
| PNG.ASICE | image/png | GESTITO |
| PNG.ASICS | image/png | GESTITO |
| PNG.P7M | image/png | GESTITO |

| | | |
|---|---|---|
| PNG.P7S | image/png | GESTITO |
| POT | application/vnd.ms-powerpoint | GESTITO |
| POT.ASICE | application/vnd.ms-powerpoint | GESTITO |
| POT.ASICS | application/vnd.ms-powerpoint | GESTITO |
| POT.P7M | application/vnd.ms-powerpoint | GESTITO |
| POT.P7S | application/vnd.ms-powerpoint | GESTITO |
| PPS | application/vnd.ms-powerpoint | GESTITO |
| PPS.ASICE | application/vnd.ms-powerpoint | GESTITO |
| PPS.ASICS | application/vnd.ms-powerpoint | GESTITO |
| PPS.P7M | application/vnd.ms-powerpoint | GESTITO |
| PPS.P7S | application/vnd.ms-powerpoint | GESTITO |
| PPSX | application/vnd.openxmlformatsofficedocument.presentationml.slideshow | IDONEO |
| PPSX.ASICE | application/vnd.openxmlformatsofficedocument.presentationml.slideshow | IDONEO |
| PPSX.ASICS | application/vnd.openxmlformatsofficedocument.presentationml.slideshow | IDONEO |
| PPSX.P7M | application/vnd.openxmlformatsofficedocument.presentationml.slideshow | IDONEO |
| PPSX.P7S | application/vnd.openxmlformatsofficedocument.presentationml.slideshow | IDONEO |

| | | |
|---|---|---|
| PPT | application/vnd.ms-powerpoint | GESTITO |
| PPT.ASICE | application/vnd.ms-powerpoint | GESTITO |
| PPT.ASICS | application/vnd.ms-powerpoint | GESTITO |
| PPT.P7M | application/vnd.ms-powerpoint | GESTITO |
| PPT.P7S | application/vnd.ms-powerpoint | GESTITO |
| PPTM | application/vnd.ms-powerpoint.presentation.macroenabled.12 | GESTITO |
| PPTM.ASICE | application/vnd.ms-powerpoint.presentation.macroenabled.12 | GESTITO |
| PPTM.ASICS | application/vnd.ms-powerpoint.presentation.macroenabled.12 | GESTITO |
| PPTM.P7M | application/vnd.ms-powerpoint.presentation.macroenabled.12 | GESTITO |
| PPTM.P7S | application/vnd.ms-powerpoint.presentation.macroenabled.12 | GESTITO |
| PPTX | application/vnd.openxmlformats-officedocument.presentationml.presentation | GESTITO |
| PPTX.ASICE | application/vnd.openxmlformats-officedocument.presentationml.presentation | GESTITO |
| PPTX.ASICS | application/vnd.openxmlformats-officedocument.presentationml.presentation | GESTITO |
| PPTX.P7M | application/vnd.openxmlformats-officedocument.presentationml.presentation | GESTITO |

| | | |
|---|---|---|
| PPTX.P7S | application/vnd.openxmlformats-officedocument.presentationml.presentation | GESTITO |
| PRJ | text/plain | GESTITO |
| PRJ.ASICE | text/plain | GESTITO |
| PRJ.ASICS | text/plain | GESTITO |
| PRJ.P7M | text/plain | GESTITO |
| PRJ.P7S | text/plain | GESTITO |
| PSD | image/vnd.adobe.photoshop | GESTITO |
| PSD.ASICE | image/vnd.adobe.photoshop | GESTITO |
| PSD.ASICS | image/vnd.adobe.photoshop | GESTITO |
| PSD.P7M | image/vnd.adobe.photoshop | GESTITO |
| PSD.P7S | image/vnd.adobe.photoshop | GESTITO |
| PUB | application/x-mspublisher | GESTITO |
| PUB.ASICE | application/x-mspublisher | GESTITO |
| PUB.ASICS | application/x-mspublisher | GESTITO |
| PUB.P7M | application/x-mspublisher | GESTITO |
| PUB.P7S | application/x-mspublisher | GESTITO |
| RAR | application/x-rar-compressed | GESTITO |
| RAR.ASICE | application/x-rar-compressed | GESTITO |

| | | |
|---|---|---|
| RAR.ASICS | application/x-rar-compressed | GESTITO |
| RAR.P7M | application/x-rar-compressed | GESTITO |
| RAR.P7S | application/x-rar-compressed | GESTITO |
| RTF | application/rtf | GESTITO |
| RTF.ASICE | application/rtf | GESTITO |
| RTF.ASICS | application/rtf | GESTITO |
| RTF.P7M | application/rtf | GESTITO |
| RTF.P7S | application/rtf | GESTITO |
| SBN | application/octet-stream | GESTITO |
| SBN.ASICE | application/octet-stream | GESTITO |
| SBN.ASICS | application/octet-stream | GESTITO |
| SBN.P7M | application/octet-stream | GESTITO |
| SBN.P7S | application/octet-stream | GESTITO |
| SBX | application/octet-stream | GESTITO |
| SBX.ASICE | application/octet-stream | GESTITO |
| SBX.ASICS | application/octet-stream | GESTITO |
| SBX.P7M | application/octet-stream | GESTITO |
| SBX.P7S | application/octet-stream | GESTITO |
| SDC | application/vnd.stardivision.calc | IDONEO |

| | | |
|---|---|---|
| SDC.ASICE | application/vnd.stardivision.calc | IDONEO |
| SDC.ASICS | application/vnd.stardivision.calc | IDONEO |
| SDC.P7M | application/vnd.stardivision.calc | IDONEO |
| SDC.P7S | application/vnd.stardivision.calc | IDONEO |
| SGP | text/plain | IDONEO |
| SGP.ASICE | text/plain | IDONEO |
| SGP.ASICS | text/plain | IDONEO |
| SGP.P7M | text/plain | IDONEO |
| SGP.P7S | text/plain | IDONEO |
| SHP | application/octet-stream | GESTITO |
| SHP.ASICE | application/octet-stream | GESTITO |
| SHP.ASICS | application/octet-stream | GESTITO |
| SHP.P7M | application/octet-stream | GESTITO |
| SHP.P7S | application/octet-stream | GESTITO |
| SHX | application/octet-stream | GESTITO |
| SHX.ASICE | application/octet-stream | GESTITO |
| SHX.ASICS | application/octet-stream | GESTITO |
| SHX.P7M | application/octet-stream | GESTITO |
| SHX.P7S | application/octet-stream | GESTITO |

| | | |
|---|---|---|
| SITX | application/x-stuffit | IDONEO |
| SITX.ASICE | application/x-stuffit | IDONEO |
| SITX.ASICS | application/x-stuffit | IDONEO |
| SITX.P7M | application/x-stuffit | IDONEO |
| SITX.P7S | application/x-stuffit | IDONEO |
| SVG | image/svg+xml | IDONEO |
| SVG.ASICE | image/svg+xml | IDONEO |
| SVG.ASICS | image/svg+xml | IDONEO |
| SVG.P7M | image/svg+xml | IDONEO |
| SVG.P7S | image/svg+xml | IDONEO |
| SWF | application/x-shockwave-flash | GESTITO |
| SWF.ASICE | application/x-shockwave-flash | GESTITO |
| SWF.ASICS | application/x-shockwave-flash | GESTITO |
| SWF.P7M | application/x-shockwave-flash | GESTITO |
| SWF.P7S | application/x-shockwave-flash | GESTITO |
| SXC | application/vnd.sun.xml.calc | GESTITO |
| SXC.ASICE | application/vnd.sun.xml.calc | GESTITO |
| SXC.ASICS | application/vnd.sun.xml.calc | GESTITO |
| SXC.P7M | application/vnd.sun.xml.calc | GESTITO |

| | | |
|---|---|---|
| SXC.P7S | application/vnd.sun.xml.calc | GESTITO |
| SXW | application/vnd.sun.xml.writer | GESTITO |
| SXW.ASICE | application/vnd.sun.xml.writer | GESTITO |
| SXW.ASICS | application/vnd.sun.xml.writer | GESTITO |
| SXW.P7M | application/vnd.sun.xml.writer | GESTITO |
| SXW.P7S | application/vnd.sun.xml.writer | GESTITO |
| TAR | application/x-gtar | GESTITO |
| TAR.ASICE | application/x-gtar | GESTITO |
| TAR.ASICS | application/x-gtar | GESTITO |
| TAR.P7M | application/x-gtar | GESTITO |
| TAR.P7S | application/x-gtar | GESTITO |
| TEXTCLIPPING | application/octet-stream | GESTITO |
| TEXTCLIPPING.ASICE | application/octet-stream | GESTITO |
| TEXTCLIPPING.ASICS | application/octet-stream | GESTITO |
| TEXTCLIPPING.P7M | application/octet-stream | GESTITO |
| TEXTCLIPPING.P7S | application/octet-stream | GESTITO |
| THMX | application/vnd.openxmlformats-officedocument | GESTITO |
| THMX.ASICE | application/vnd.openxmlformats-officedocument | GESTITO |
| THMX.ASICS | application/vnd.openxmlformats-officedocument | GESTITO |

| | | |
|---|---|---|
| THMX.P7M | application/vnd.openxmlformats-officedocument | GESTITO |
| THMX.P7S | application/vnd.openxmlformats-officedocument | GESTITO |
| TIF | image/tiff | IDONEO |
| TIF.ASICE | image/tiff | IDONEO |
| TIF.ASICS | image/tiff | IDONEO |
| TIF.P7M | image/tiff | IDONEO |
| TIF.P7S | image/tiff | IDONEO |
| TIFF | image/tiff | IDONEO |
| TIFF.ASICE | image/tiff | IDONEO |
| TIFF.ASICS | image/tiff | IDONEO |
| TIFF.P7M | image/tiff | IDONEO |
| TIFF.P7S | image/tiff | IDONEO |
| TSD | application/timestamped-data | GESTITO |
| TSR | application/timestamp-reply | GESTITO |
| TSR.ASICE | application/timestamp-reply | GESTITO |
| TSR.ASICS | application/timestamp-reply | GESTITO |
| TSR.P7M | application/timestamp-reply | GESTITO |
| TSR.P7S | application/timestamp-reply | GESTITO |
| TXT | text/plain | IDONEO |

| | | |
|---|---|---|
| TXT.ASICE | text/plain | IDONEO |
| TXT.ASICS | text/plain | IDONEO |
| TXT.P7M | text/plain | IDONEO |
| TXT.P7S | text/plain | IDONEO |
| UNKNOWN | parer/unknonwn | DEPRECATO |
| VCF | text/x-vcard | GESTITO |
| VCF.ASICE | text/x-vcard | GESTITO |
| VCF.ASICS | text/x-vcard | GESTITO |
| VCF.P7M | text/x-vcard | GESTITO |
| VCF.P7S | text/x-vcard | GESTITO |
| VSDX | application/vnd.ms-visio.drawing.main+xml | GESTITO |
| VSDX.ASICE | application/vnd.ms-visio.drawing.main+xml | GESTITO |
| VSDX.ASICS | application/vnd.ms-visio.drawing.main+xml | GESTITO |
| VSDX.P7M | application/vnd.ms-visio.drawing.main+xml | GESTITO |
| VSDX.P7S | application/vnd.ms-visio.drawing.main+xml | GESTITO |
| WEBARCHIVE | application/x-bplist | GESTITO |
| WEBARCHIVE.ASICE | application/x-bplist | GESTITO |
| WEBARCHIVE.ASICS | application/x-bplist | GESTITO |
| WEBARCHIVE.P7M | application/x-bplist | GESTITO |

| | | |
|---|---|---|
| WEBARCHIVE.P7S | application/x-bplist | GESTITO |
| WMZ | application/x-ms-wmz | GESTITO |
| WMZ.ASICE | application/x-ms-wmz | GESTITO |
| WMZ.ASICS | application/x-ms-wmz | GESTITO |
| WMZ.P7M | application/x-ms-wmz | GESTITO |
| WMZ.P7S | application/x-ms-wmz | GESTITO |
| WPS | application/vnd.ms-works | GESTITO |
| WPS.ASICE | application/vnd.ms-works | GESTITO |
| WPS.ASICS | application/vnd.ms-works | GESTITO |
| WPS.P7M | application/vnd.ms-works | GESTITO |
| WPS.P7S | application/vnd.ms-works | GESTITO |
| XBRL | application/xbrl-instance+xml | GESTITO |
| XBRL.ASICE | application/xbrl-instance+xml | GESTITO |
| XBRL.ASICS | application/xbrl-instance+xml | GESTITO |
| XBRL.P7M | application/xbrl-instance+xml | GESTITO |
| XBRL.P7S | application/xbrl-instance+xml | GESTITO |
| XCF | image/x-xcf | GESTITO |
| XCF.ASICE | image/x-xcf | GESTITO |
| XCF.ASICS | image/x-xcf | GESTITO |

| | | |
|---|---|---|
| XCF.P7M | image/x-xcf | GESTITO |
| XCF.P7S | image/x-xcf | GESTITO |
| XHT | application/xhtml+xml | GESTITO |
| XHT.ASICE | application/xhtml+xml | GESTITO |
| XHT.ASICS | application/xhtml+xml | GESTITO |
| XHT.P7M | application/xhtml+xml | GESTITO |
| XHT.P7S | application/xhtml+xml | GESTITO |
| XHTML | application/xhtml+xml | GESTITO |
| XHTML.ASICE | application/xhtml+xml | GESTITO |
| XHTML.ASICS | application/xhtml+xml | GESTITO |
| XHTML.P7M | application/xhtml+xml | GESTITO |
| XHTML.P7S | application/xhtml+xml | GESTITO |
| XLS | application/vnd.ms-excel | GESTITO |
| XLS.ASICE | application/vnd.ms-excel | GESTITO |
| XLS.ASICS | application/vnd.ms-excel | GESTITO |
| XLS.P7M | application/vnd.ms-excel | GESTITO |
| XLS.P7S | application/vnd.ms-excel | GESTITO |
| XLSB | application/vnd.ms-excel.sheet.binary.macroenabled.12 | GESTITO |
| XLSB.ASICE | application/vnd.ms-excel.sheet.binary.macroenabled.12 | GESTITO |

| | | |
|---|---|---|
| XLSB.ASICS | application/vnd.ms-excel.sheet.binary.macroenabled.12 | GESTITO |
| XLSB.P7M | application/vnd.ms-excel.sheet.binary.macroenabled.12 | GESTITO |
| XLSB.P7S | application/vnd.ms-excel.sheet.binary.macroenabled.12 | GESTITO |
| XLSM | application/vnd.ms-excel.sheet.macroenabled.12 | GESTITO |
| XLSM.ASICE | application/vnd.ms-excel.sheet.macroenabled.12 | GESTITO |
| XLSM.ASICS | application/vnd.ms-excel.sheet.macroenabled.12 | GESTITO |
| XLSM.P7M | application/vnd.ms-excel.sheet.macroenabled.12 | GESTITO |
| XLSM.P7S | application/vnd.ms-excel.sheet.macroenabled.12 | GESTITO |
| XLSX | application/vnd.openxmlformatsofficedocument.spreadsheetml.sheet | GESTITO |
| XLSX.ASICE | application/vnd.openxmlformatsofficedocument.spreadsheetml.sheet | GESTITO |
| XLSX.ASICS | application/vnd.openxmlformatsofficedocument.spreadsheetml.sheet | GESTITO |
| XLSX.P7M | application/vnd.openxmlformatsofficedocument.spreadsheetml.sheet | GESTITO |
| XLSX.P7S | application/vnd.openxmlformatsofficedocument.spreadsheetml.sheet | GESTITO |
| XLTX | application/vnd.openxmlformatsofficedocument.spreadsheetml.template | GESTITO |
| XLTX.ASICE | application/vnd.openxmlformatsofficedocument.spreadsheetml.template | GESTITO |

| | | |
|---|---|---|
| XLTX.ASICS | application/vnd.openxmlformatsofficedocument.spreadsheetml.template | GESTITO |
| XLTX.P7M | application/vnd.openxmlformatsofficedocument.spreadsheetml.template | GESTITO |
| XLTX.P7S | application/vnd.openxmlformatsofficedocument.spreadsheetml.template | GESTITO |
| XML | application/xml | IDONEO |
| XML.ASICE | application/xml | IDONEO |
| XML.ASICS | application/xml | IDONEO |
| XML.P7M | application/xml | IDONEO |
| XML.P7S | application/xml | IDONEO |
| XPS | application/vnd.ms-xpsdocument | GESTITO |
| XPS.ASICE | application/vnd.ms-xpsdocument | GESTITO |
| XPS.ASICS | application/vnd.ms-xpsdocument | GESTITO |
| XPS.P7M | application/vnd.ms-xpsdocument | GESTITO |
| XPS.P7S | application/vnd.ms-xpsdocument | GESTITO |
| XSD | application/xml | IDONEO |
| XSD.ASICE | application/xml | IDONEO |
| XSD.ASICS | application/xml | IDONEO |
| XSD.P7M | application/xml | IDONEO |

| | | |
|---|---|---|
| XSD.P7S | application/xml | IDONEO |
| XSL | application/xml | IDONEO |
| XSL-FO | application/xslfo+xml | IDONEO |
| XSL-FO.ASICE | application/xslfo+xml | IDONEO |
| XSL-FO.ASICS | application/xslfo+xml | IDONEO |
| XSL-FO.P7M | application/xslfo+xml | IDONEO |
| XSL-FO.P7S | application/xslfo+xml | IDONEO |
| XSL.ASICE | application/xml | IDONEO |
| XSL.ASICS | application/xml | IDONEO |
| XSL.P7M | application/xml | IDONEO |
| XSL.P7S | application/xml | IDONEO |
| XSLFO | application/xslfo+xml | IDONEO |
| XSLFO.ASICE | application/xslfo+xml | IDONEO |
| XSLFO.ASICS | application/xslfo+xml | IDONEO |
| XSLFO.P7M | application/xslfo+xml | IDONEO |
| XSLFO.P7S | application/xslfo+xml | IDONEO |
| XSLT | application/xslt+xml | IDONEO |
| XSLT.ASICE | application/xslt+xml | IDONEO |
| XSLT.ASICS | application/xslt+xml | IDONEO |

| | | |
|---|---|---|
| XSLT.P7M | application/xslt+xml | IDONEO |
| XSLT.P7S | application/xslt+xml | IDONEO |
| ZIP | application/zip | IDONEO |
| ZIP.ASICE | application/zip | IDONEO |
| ZIP.ASICS | application/zip | IDONEO |
| ZIP.P7M | application/zip | IDONEO |
| ZIP.P7S | application/zip | IDONEO |

**Tabella Formati**

## Tipi oggetto da trasformare

Per oggetto da trasformare si intende un insieme di uno o più documenti che per ragioni di natura tecnica e organizzativa non è possibile produrre nel formato di SIP standard da trasmettere direttamente al Sistema di conservazione.
In tali casi il processo di conservazione prevede una fase di Preacquisizione che ha in input un oggetto da trasformare dall'Ente e in output uno o più SIP standard da versare a Sacer.
La tabella Tipi oggetto da trasformare elenca i tipi oggetto da trasformare restituendo per ciascuno l'informazione relativa al Versatore dell'oggetto, alla Trasformazione utilizzata e il tipo oggetto contenente i SIP standard da versare a Sacer.

## Gestione dei SIP rifiutati

Il Sistema registra i SIP il cui versamento è fallito in un'area temporanea del Sistema. Tali SIP sono conservati nel Sistema secondo le seguenti politiche:

- i SIP relativi a versamenti falliti e successivamente andati a buon fine (c.d. errori risolti), sono conservati nel Sistema per un anno dal loro tentato versamento;
- i SIP relativi a versamenti falliti che non saranno più ritentati (c.d. errori non risolubili), sono conservati nel Sistema per un anno dal loro tentato versamento;
- i SIP relativi a versamenti falliti non risolti e non indicati come non risolubili, per i quali è identificata la Struttura versante, la chiave e la tipologia di unità documentaria, sono conservati nel Sistema per un anno dal momento in cui tutte le aggregazioni documentali previste per quella specifica tipologia di unità documentaria per l'anno indicato nella chiave del SIP sono state chiuse e prese in custodia;
- i SIP relativi a versamenti falliti non risolti e non indicati come non risolubili, per i quali non è possibile identificare l'anno e/o la tipologia di unità documentaria e/o la Struttura versante, sono conservati per un anno dal tentato versamento.

Per ulteriori informazioni in merito alle modalità di rifiuto o accettazione dei SIP trasmessi, si rinvia al Manuale, al documento Specifiche tecniche dei servizi di versamento e al documento Codifiche errori in cui sono descritti gli errori restituiti dal Sistema a fronte delle operazioni di versamento, recupero e annullamento effettuate utilizzando i web service.

## Generazione delle Serie documentarie

Le unità documentarie acquisite nel Sistema di conservazione sono selezionabili per essere aggregate in Serie di unità documentarie.
Il criterio "standard" di generazione delle serie definito da ParER è basato su tre elementi:

- Anno di produzione/repertoriazione dell'unità documentaria;
- Tipologia di unità documentaria;
- Registro

In accordo con l'Ente è prevista la possibilità di configurare criteri specifici per la generazione di serie di unità documentarie che non rientrano nei criteri standard, utilizzando, ad esempio, un metadato specifico o un particolare tipo di documento.
Inoltre, è prevista per l'Ente la possibilità di comunicare la consistenza della serie specificando ad esempio il numero complessivo delle unità documentarie che appartengono alla serie o l'eventuale presenza di lacune. L'Ente può comunicare tali informazioni utilizzando apposite funzionalità del Sistema.
Il processo di generazione della serie si conclude con la sua validazione definitiva da parte del Responsabile della funzione archivistica di conservazione di ParER e la generazione del relativo pacchetto di archiviazione (d'ora in poi AIP) di livello serie.
I tipi serie eventualmente configurati sono indicati nella Tabella Elenco tipi serie.

## Modalità di annullamento dei versamenti

Nel caso in cui un versamento andato a buon fine sia stato effettuato per errore o contenga degli errori non correggibili altrimenti, l'Ente provvede ad annullarlo utilizzando apposite funzionalità del Sistema oppure inviando al personale di ParER una richiesta formale completa degli estremi dei documenti da annullare e relativa motivazione.
Gli oggetti non sono cancellati dal Sistema ma marcati come Annullati e sono comunque sempre consultabili tramite l'apposita sezione di ricerca.

## Modalità di restituzione degli oggetti versati in conservazione in caso di recesso

ParER garantisce il mantenimento nel proprio Sistema dei Documenti informatici e delle Aggregazioni documentali informatiche conservati, con i metadati a essi associati e le evidenze informatiche generate nel corso del processo di conservazione fino alla comunicazione da parte dell'Ente dell'effettiva messa a disposizione del Sistema in cui effettuare il riversamento.
ParER provvederà all'eliminazione dal proprio Sistema di tutti gli oggetti riversati e di tutti gli elementi riferiti all'Ente solo al termine del riversamento e solo dopo le opportune verifiche - effettuate da entrambe le Parti e svolte di concerto tra le stesse – di corretto svolgimento del riversamento stesso. In tal caso viene garantita la completa cancellazione e non leggibilità dei dati.
L'intera operazione dovrà comunque avvenire con l'autorizzazione e la vigilanza delle competenti autorità, in particolare delle strutture del MIBACT.
In caso di chiusura del servizio da parte della Regione Emilia-Romagna, con interventi di modifica alla normativa regionale, si provvederà a trasferire quanto conservato al Sistema individuato per proseguire le attività. Per quanto riguarda gli aspetti operativi per il trasferimento di archivi ad altri sistemi di conservazione, ParER adotta lo standard Uni Sincro, e provvederà a trasferire secondo canali sicuri concordati con l'Ente o con il nuovo Conservatore le informazioni. Analogamente il Sistema è predisposto per la ricezione di archivi in formato Uni Sincro; qualora il precedente sistema di conservazione non sia in grado di produrre l'archivio in formato Uni Sincro, ParER, a seguito di specifici accordi, può mettere a disposizione dell'Ente consulenza e strumenti per facilitare il trasferimento dell'archivio.

# LegalDoc

## ALLEGATO TECNICO AL CONTRATTO

InfoCert
TINEXTA GROUP

## SOMMARIO

## 1. NOVITÀ INTRODOTTE RISPETTO ALLA PRECEDENTE EMISSIONE

| | | | |
|---|---|---|---|
| Versione/Release n° | 1.3 | Data Versione/Release | novembre 2020 |
| Descrizione Modifiche | Ampliamento servizi di storage | | |

| | | | |
|---|---|---|---|
| Versione/Release n° | 1.2 | Data Versione/Release | ottobre 2020 |
| Descrizione Modifiche | Nuovo template<br>Localizzazione DR in Italia | | |

| | | | |
|---|---|---|---|
| Versione/Release n° | 1.0 | Data Versione/Release | 2013 |
| Descrizione Modifiche | Prima emissione | | |

## 2. INTRODUZIONE

Questo documento costituisce l'Allegato Tecnico alle "Condizioni generali di Contratto per l'uso del servizio LegalDoc in modalità A.S.P.", più brevemente denominato "Contratto".

Scopo di questo documento è di integrare e precisare i termini e le condizioni d'uso del servizio LegalDoc già descritti nel "Contratto", ai cui articoli è fatto esplicito riferimento.

LegalDoc è una procedura informatica per la conservazione dei documenti informatici in ottemperanza al Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013, ai sensi del Codice dell'Amministrazione Digitale, del Decreto Ministero dell'Economia e delle Finanze del 17 giugno 2014 e delle Linee Guida AgID su formazione gestione e conservazione dei documenti informatici.

Il Servizio è reso in modalità A.S.P. (*Application Service Providing*) e consente al Cliente di accedere ai servizi di conservazione di propri documenti informatici su un elaboratore elettronico, gestito da InfoCert.

Il Servizio è accessibile dall'apposita URL di rete:
**https://conservazione.infocert.it/ws/**

## 3. IL SERVIZIO

### FUNZIONI

LegalDoc consente la conservazione di documenti informatici, anche firmati digitalmente, e la riproduzione dei documenti conservati.

Il servizio permette al Cliente:

- la conservazione, tramite invio telematico, di un documento analogico opportunamente digitalizzato o di un documento informatico
- la rettifica per via telematica di un documento già conservato
- la cancellazione per via telematica di un documento già conservato
- l'esibizione per via telematica di un documento già conservato
- il caricamento per via telematica dei visualizzatori dei documenti
- la conservazione degli indici di ricerca associati al documento
- la ricerca di un documento in base agli indici associati
- la delega ad InfoCert della responsabilità del procedimento, che comporta anche l'apposizione della marca temporale, della firma di controllo del procedimento effettuata tramite tecnologie di firma digitale e marcatura temporale digitale
- gli adempimenti previsti dalla normativa relativi alla sicurezza fisica e logica dell'archivio dei documenti conservati e dell'intero procedimento di conservazione
- la conservazione presso InfoCert di tutti i documenti inviati per la conservazione
- la conservazione, la rettifica, la cancellazione e l'esibizione di documenti contabili con effetto anche ai fini fiscali nei casi previsti
- l'invio automatico di documenti gestiti da LegalDoc via posta elettronica certificata (opzionale)
- la firma automatica e la marcatura temporale di documenti (opzionale).

### MODALITÀ D'ESECUZIONE E D'ACCESSO

I requisiti per accedere al Servizio sono:

- aver sottoscritto le Condizioni Generali d'adesione al servizio in A.S.P. ed il Modulo di Richiesta Attivazione
- essere titolari delle credenziali di accesso (fornite in sede contrattuale)
- essere titolari di una casella di posta certificata

- possedere gli strumenti tecnici necessari (hardware, software e collegamenti telematici aventi le caratteristiche di seguito meglio descritte) per il collegamento all'URL dove risiede il Servizio;

Il Cliente s'impegna per l'attivazione del servizio a fornire ad InfoCert tutte le informazioni necessarie alla configurazione del sistema, previste nell'apposito documento allegato "*Scheda Dati Tecnici per l'attivazione di LegalDoc*".

I servizi LegalDoc sono invocati dal Sistema del Cliente tramite la tecnologia Web Services, secondo il paradigma REST.

L'accesso avviene tramite collegamento all'URL sopra indicata e deve prevedere un unico canale di trasmissione dei documenti. Nel servizio LegalDoc non sono permessi invii in multithread.

Una procedura informatica d'identificazione permette al Sistema del Cliente d'identificarsi per inviare ad InfoCert i documenti da conservare e per richiedere in esibizione i documenti conservati. Tale procedura prevede la comunicazione, da parte del Cliente, delle credenziali di accesso e fornisce al Cliente un identificativo temporaneo detto identificativo di sessione.

In seguito all'esito positivo della procedura d'identificazione tutte le operazioni si considerano effettuate dal Sistema del Cliente, che è obbligato ad osservare la massima diligenza nell'utilizzo, conservazione e protezione delle credenziali di accesso e dell'identificativo di sessione.

In considerazione di quanto stabilito al periodo precedente, InfoCert non potrà essere ritenuta responsabile, salvo il caso di dolo o colpa grave, per eventuali danni derivanti al Cliente dal compimento di dette operazioni.

Il Cliente s'impegna a richiamare i servizi di LegalDoc dal proprio Sistema secondo le modalità indicate nel documento allegato: "*Specifiche tecniche per l'integrazione di LegalDoc*".

In particolare, InfoCert non procederà alla conservazione dei documenti inviati:

- che non siano accompagnati dal file dei parametri di conservazione e dal file degli indici, entrambi in formato XML
- in cui tali file siano in formato non corretto o mancanti delle informazioni obbligatorie richieste per l'operazione di conservazione o di rettifica
- i cui file componenti non siano dei formati (MIME Type) ammessi alla conservazione e specificati nella "*Scheda Dati Tecnici per l'attivazione di LegalDoc*"

I formati 'standard' proposti sono:

| **Formato** | Estensione | MIME-Type | Standard |
|---|---|---|---|
| **PDF o PDF/A** | .pdf | application/pdf;NA | ISO 32000-1 (PDF), ISO 19005-1:2005 (vers. PDF 1.4), ISO 19005-2:2011 (vers. PDF 1.7) |

| Formato | Estensione | MIME-Type | Standard |
|---|---|---|---|
| **TIFF** | .tif | image/tiff;NA | ISO 12639(TIFF/IT); ISO 12234 (TIFF/EP) |
| **XML** | .xml | text/xml;1.0 | |
| **TXT** | .txt | text/plain;NA | |

Il Cliente s'impegna altresì ad avere depositato presso InfoCert, precedentemente l'invio dei relativi file, il relativo software per la visualizzazione/stampa (viewer) dei formati non standard. I formati sono definiti "*Scheda Dati Tecnici per l'attivazione di LegalDoc*".

I campi del file di indice che richiedono un controllo di obbligatorietà per le classi documentali standard sono definiti nella "*Scheda Dati Tecnici per l'attivazione di LegalDoc*". Per gli indici obbligatori, deve essere utilizzata la denominazione fornita da InfoCert.

La denominazione degli indici non obbligatori può essere liberamente inserita dal Cliente. Sarà poi onere del Cliente utilizzare, in fase di ricerca, la stessa denominazione inserita in fase di conservazione.
La struttura della denominazione ha le limitazioni espresse nelle "*Specifiche tecniche per l'integrazione di LegalDoc*".

Il Cliente s'impegna ad attivare una o più policy, ovvero regole di comportamento personalizzate che specificano le regole per l'accesso al parco documentale, i tipi di documento che si possono inviare in conservazione e i parametri di conservazione.
InfoCert non sarà in alcun modo responsabile del contenuto dei documenti inviati dal Sistema del Cliente (virus, contenuto ecc.), né dei dati indicati dal Cliente nel file XML dei parametri e nel file XML degli indici usati per l'indicizzazione e la classificazione del documento nel processo di conservazione.

Per ogni documento accettato dal sistema LegalDoc, sono ritornati al Sistema mittente tramite Web Services rispettivamente:

- un codice (descritto nelle "*Specifiche Tecniche di Integrazione*") che indica l'esito dell'operazione
- il file XML Indice di Conservazione (IdC) contenente l'identificativo univoco del documento conservato e gli hash dei file controllati da LegalDoc. A questo file sono apposte firma digitale e marcatura temporale da parte del Responsabile del servizio della conservazione.

È a cura del Cliente la memorizzazione delle informazioni contenute nell'Indice di Conservazione che sono utilizzate per successive richieste al sistema LegalDoc riguardanti il documento conservato.

Eventuali codici di errore sono specificati nel documento "Descrizione dei codici di errore".

Non esistono limiti massimi di rifiuti nei tentativi di versamento.

### UTILIZZO DEL SERVIZIO DI POSTA ELETTRONICA INTEGRATA (OPZIONALE)

Il Cliente ha la possibilità di richiedere la configurazione di una casella di posta elettronica certificata al fine di trasmettere, in modo automatico, le fatture elettroniche o altri documenti gestiti dal servizio LegalDoc ai destinatari indicati nel file degli indici.

È responsabilità del Cliente, pertanto, definire correttamente gli indirizzi di posta elettronica dei destinatari.

È completa cura del Cliente, altresì, la gestione della casella di posta elettronica in dotazione (ricezione avvisi di consegna e/o mancato recapito, conservazione delle ricevute, verifica spazio disponibile, etc.).

Per l'utilizzo di posta elettronica certificata il Cliente prende atto dell'applicazione delle relative norme di legge, e, in particolare, del D.P.R. n. 68/2005 e delle regole tecniche di cui al D.M. 2.11.2005 e delle relative condizioni di servizio InfoCert.

### UTILIZZO DEL SERVIZIO DI FIRMA AUTOMATICA (OPZIONALE)

Il Cliente ha la possibilità di richiedere l'attivazione, all'interno dell'applicazione LegalDoc, del servizio di firma automatica dei documenti.

La soluzione permette di apporre tramite LegalDoc firme digitali, secondo le relative condizioni di servizio InfoCert.

### UTILIZZO DEL SERVIZIO DI MARCATURA TEMPORALE (OPZIONALE)

Il Cliente ha la possibilità di richiedere l'attivazione, all'interno della applicazione LegalDoc, del servizio InfoCert di marcatura temporale. Il cliente può richiedere l'applicazione della marca temporale su tutti i documenti di una o più tipologie documentali; InfoCert provvede alla marcatura temporale contestualmente alla firma digitale dei documenti, secondo le relative condizioni del servizio InfoCert. Il servizio è applicabile anche a procedure di apposizione di "Data Certa".

## 4. ATTIVITÀ DI SUPPORTO

Il servizio è comprensivo di un supporto erogato da InfoCert nei seguenti termini:

- call-center incaricato dell'assistenza al cliente raggiungibile tramite telefono al numero **800.777.579**
  servizio disponibile nei seguenti orari: lunedì – venerdì dalle 8.30 alle 19.00, eccetto i festivi
- ticket https://help.infocert.it/

## 5. LIVELLI DI SERVIZIO

### MODALITÀ DI EROGAZIONE

Nel verificare la disponibilità dell'erogazione e, di conseguenza, nel calcolo del livello di servizio, InfoCert considera soltanto le componenti di propria competenza. La figura sottostante (FIG. 1) offre uno schema esemplificativo del dialogo tra l'applicazione del Cliente ed il servizio di conservazione dei documenti LegalDoc, allo scopo di distinguere le parti che rimarranno sotto la responsabilità di InfoCert da quelle di competenza esclusiva del Cliente.

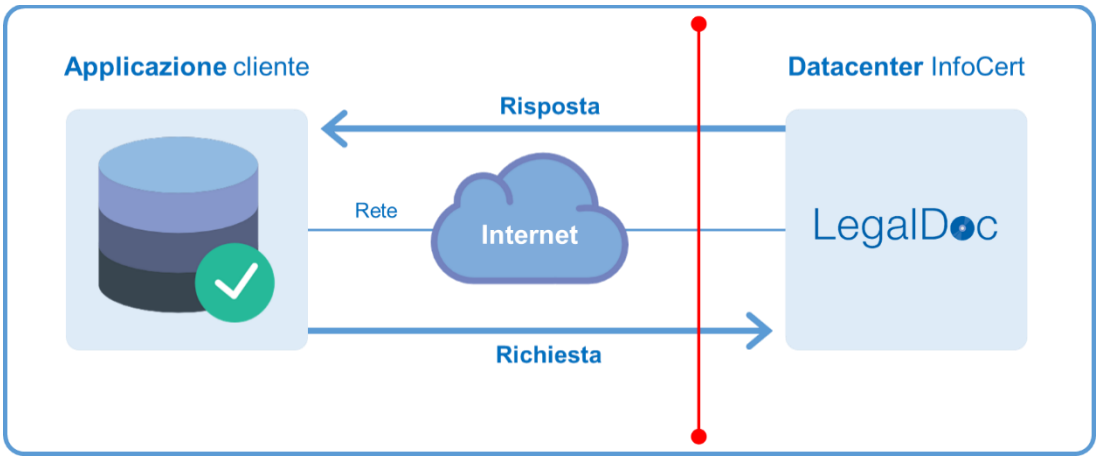


**FIG. 1 architettura generale**

Alla luce dello schema sopra riportato (FIG. 1), InfoCert non è ritenuta responsabile per le performance della rete Internet attraverso la quale si effettua la richiesta verso il suo Data Center (nella fig. *rete*); inoltre, sarà di responsabilità del Cliente il corretto funzionamento dell'applicazione utilizzata per richiamare le funzionalità LegalDoc (nella fig. *Applicazione Cliente*).

Per **richiesta** si intenderà l'invocazione delle funzionalità di invio in *conservazione* del documento, *cancellazione* del documento, *rettifica* del documento, *esibizione* del documento.

Per **risposta** del servizio LegalDoc si intenderà l'invio all'Applicazione Cliente, a seguito di una richiesta, del messaggio HTTP comprendente il codice che indica il risultato dell'operazione e gli altri file di corredo, così come specificato nei manuali "*Specifiche tecniche per l'integrazione di LegalDoc*" e "*Descrizione dei codici di errore di LegalDoc*".

### SERVICE LEVEL AGREEMENT

InfoCert, entro 10 giorni lavorativi dall'attivazione del contratto e dalla verifica dei dati indicati dal Cliente nella *"Scheda Dati Tecnici per l'attivazione di LegalDoc",* provvede ad assegnare al Cliente un profilo d'abilitazione per l'accesso al Servizio e a fornire le credenziali di accesso necessarie.

InfoCert avrà il diritto di effettuare ogni tipo di manutenzione sui sistemi informatici, ma precisa che gli interventi di manutenzione ordinaria e straordinaria vengono effettuati, salvo caso di forza maggiore, al di fuori dell'orario di produzione.

Il Cliente, dal proprio applicativo, potrà richiamare i servizi di LegalDoc, attenendosi alle modalità indicate da InfoCert nell'apposito documento denominato "*Specifiche tecniche per l'integrazione di LegalDoc*".

Il livello di qualità del servizio di conservazione offerto da InfoCert è garantito dal rispetto dei seguenti requisiti e parametri:

1. InfoCert garantisce, per quanto concerne le componenti di propria responsabilità, una disponibilità del servizio non inferiore al 95 % dell'orario di servizio calcolata sulla base di un mese solare, a partire dal primo giorno di calendario del mese stesso;

2. sono esclusi dal Service Level Agreement tutti i casi di errata configurazione delle apparecchiature del Cliente, tutti i casi di problemi riguardanti le componenti del Cliente o la rete Internet e comunque tutti i casi di problemi riguardanti componenti che esulano dalla responsabilità di InfoCert.

In caso di criticità il servizio è presidiato dal personale incaricato nei seguenti orari: dal lunedì al venerdì, dalle ore 8:00 alle ore 21:00 ed il sabato dalle ore 8:00 fino alle ore 14:00, esclusi i giorni festivi e le festività infrasettimanali nazionali.

### CRITERI DI MISURAZIONE

Il Service Level Management (SLM) previsto per questo servizio è regolato da un'unica metrica che si identifica nella **"disponibilità".**

Il calcolo della disponibilità del servizio viene effettuato facendo riferimento ai minuti di indisponibilità effettivi del servizio nell'orario di produzione concordato, secondo quanto indicato dall'**art. 4.2 Responsabilità di InfoCert** delle Condizioni Generali del Contratto e dal presente Allegato Tecnico.

InfoCert verifica il corretto funzionamento dei servizi tramite l'utilizzo di strumenti software, denominate "sonde", le quali automaticamente e periodicamente simulano una richiesta di servizio da parte del Cliente.

Le specifiche di navigazione per queste sonde (es.: quali funzioni richiedere e fino a quale grado di dettaglio scendere) vengono definite da InfoCert, non contemplano attività di aggiornamento, modifica o stampa poiché eseguono automaticamente e frequentemente operazioni che simulano l'attività utente.

Qualora il servizio non risponda secondo le modalità concordate, la sonda allerta il sistema di controllo della produzione InfoCert.

L'indisponibilità del ***Servizio*** sarà dichiarata in uno dei seguenti casi:

- su segnalazione degli strumenti di monitoraggio InfoCert, previo esame e validazione da parte del sistema di controllo della produzione (Incident Management).
- su eventuale segnalazione del disservizio da parte del Cliente, previo esame e validazione da parte del sistema di controllo della produzione InfoCert. La segnalazione perviene alla funzione di Incident Management utilizzata da InfoCert, il quale registra il disservizio a partire dal momento della segnalazione del Cliente e fino al momento del ripristino del servizio.

## 6. REQUISITI SOFTWARE

Un Sistema situato presso il Cliente, in cui una procedura client costruisce i file XML dei parametri e degli indici relativi al documento da conservare ed invoca via REST i servizi LegalDoc, secondo le modalità indicate nel documento allegato: "*Specifiche tecniche per l'integrazione di LegalDoc*" facente parte degli Allegati al Contratto.

InfoCert si riserva di apportare i cambiamenti resisi necessari a questo documento e di darne tempestiva comunicazione al Cliente, che provvederà alle eventuali modifiche al proprio software client nelle modalità previste dal Contratto (**Art. 1.5 Adeguamento Manutenzione ed Aggiornamento**).

## 7. CONNETTIVITÀ

Connessione effettuata tramite collegamento ad Internet di qualsiasi tipo. Le performance del servizio sono connesse alla tipologia di connettività.

Il centro dati utilizzato da InfoCert è connesso alla rete internet con due collegamenti ATM separati entrambi con velocità massima di 155 Mbit/sec.

Tali collegamenti sono attestati su POP distinti, con percorsi fisici e apparati d'interfaccia separati e completamente ridondati.

## 8. DISPONIBILITÀ DEI DATI

InfoCert provvede alla conservazione dei documenti inviati non appena terminata la verifica sulla completezza e la correttezza delle informazioni presenti nei file XML dei parametri di conservazione e indici di ricerca secondo i parametri e le modalità indicate in dettaglio nel "*Scheda Dati Tecnici per l'attivazione di LegalDoc*" e nelle "*Specifiche tecniche per l'integrazione di LegalDoc*".

I documenti conservati sono accessibili attraverso il servizio di Esibizione.

## 9. MODALITÀ TECNICHE GENERALI DI EROGAZIONE DEL SERVIZIO

InfoCert si avvale di tre siti data center:

1. Padova
2. Modena (DR)
3. Milano (cloud privato AWS)

Nel seguito sono descritte le modalità generali tecniche e le infrastrutture che InfoCert utilizza all'interno dei propri data center.

Sia il sito primario che quello di *Disaster Recovery* sono localizzati in Italia.

### DATA CENTER DI PADOVA

#### SICUREZZA FISICA

Lo stabile che ospita i locali e i macchinari utilizzati per l'erogazione del servizio è sorvegliato da personale specializzato 24 ore al giorno; la sala CED, dove si trovano i dispositivi hardware e software dei diversi sistemi, la sala di controllo dell'alimentazione elettrica, del sistema idraulico, del condizionamento e la sala di monitoraggio dei sistemi di sicurezza installati, è accessibile solo mediante utilizzo di *badge* autorizzato ed è controllato da un sistema TVCC; le porte sono dotate d'allarmi a contatti magnetici; le stanze dell'area sono controllate mediante rivelatori combinati microonde e infrarossi.

Le aree del CED sono dotate d'impianto di rilevazione fumi e antincendio.

#### ALIMENTAZIONE ELETTRICA - GARANZIA GRUPPI DI CONTINUITÀ

Tutte le apparecchiature del centro dati sono collegate alla rete elettrica attraverso gruppi di continuità che consentono di mantenere l'alimentazione alle apparecchiature in caso d'interruzione dell'erogazione dell'energia elettrica da parte del fornitore. In caso d'assenza dell'alimentazione per pochi cicli, intervengono automaticamente delle batterie tampone in grado di mantenere la continuità elettrica. Qualora l'assenza di alimentazione si protragga per più di pochi secondi, vengono automaticamente avviati dei gruppi elettrogeni che iniziano a fornire l'alimentazione al gruppo di continuità.

#### CONNESSIONE AD INTERNET

Il centro dati utilizzato da InfoCert è connesso alla rete Internet con due collegamenti ATM separati entrambi con velocità massima di 155 Mbit/sec.

Tali collegamenti sono attestati su POP distinti, con percorsi fisici e apparati d'interfaccia separati e completamente ridondati.

I tempi d'attraversamento rete tra il Centro Servizi ed i nodi d'interconnessione con i principali Provider italiani ed internazionali sono estremamente contenuti (inferiori a 20 ms).

### SICUREZZA DELLE RETI: PROTEZIONE DA INTRUSIONI

I sistemi e le reti utilizzati da InfoCert sono connessi ad Internet in modo controllato da sistemi *firewall* che consentono di suddividere la connessione in aree a sicurezza progressivamente maggiore: rete Internet, reti DMZ (Demilitarized Zone) o Perimetrali, Reti Interne. Tutto il traffico che fluisce tra le varie aree è sottoposto ad accettazione da parte del *firewall*, sulla base di un set di regole stabilite. Le regole definite sui firewall vengono progettate in base ai principi di "*default deny*" (quanto non è espressamente permesso è vietato di default, ovvero, le regole consentiranno solo quanto è strettamente necessario al corretto funzionamento dell'applicazione) e "*defense in depth*" (vengono organizzati livelli successivi di difesa, prima a livello di rete, tramite successive barriere *firewall,* ed infine a livello di sistema, *hardening).*

La definizione delle politiche d'accesso relativamente ai siti del Cliente sarà concordata, nel rispetto dei vincoli imposti dalle politiche stabilite dalla funzione Sicurezza Informatica.

I sistemi firewall utilizzati sono configurati in alta affidabilità (HA), ovvero sono formati da coppie di macchine indipendenti, collegate tra loro e gestite, tramite appositi software, in modo che in caso di guasto di una delle macchine, il traffico venga dirottato sulla macchina di backup.

### DATA CENTER AWS MILANO

A partire dal 2020 InfoCert si avvale dei servizi cloud computing Amazon Web Services (AWS) come storage sicuro.
L'infrastruttura cloud di AWS è basata su regioni e zone di disponibilità (*Availability Zone* AZ). L'AZ scelta per LegalDoc è composta da più data center, tutti in territorio italiano, provvisti di alimentazione, rete e connettività ridondanti, ognuno in una struttura separata.
Ogni regione di Amazon è pensata per essere completamente isolata dalle altre sue regioni, così da raggiungere la maggiore stabilità e tolleranza ai guasti possibile.
Il cloud AWS è certificato *Cloud Marketplace AgID* e si avvale di un modello di responsabilità condivisa (AWS ha il compito di gestire la sicurezza del cloud, InfoCert mantiene la responsabilità della sicurezza nel cloud).
L'infrastruttura è progettata e gestita secondo le *best practice* di sicurezza e nel rispetto di una serie di standard di sicurezza IT, di cui si riportano:

- SOC 1/ISAE 3402, SOC 2, SOC 3
- FISMA, DIACAP e FedRAMP
- PCI DSS livello 1
- ISO 9001, ISO 27001, ISO 27018

Infine, è attivo un servizio di crittografia dei dati a riposo e un protocollo HTTPS per i dati in transito. In dettaglio, l'algoritmo di crittografia per i CMK (*Customer Master Keys*) simmetrici è basato su *Advanced Encryption Standard* (AES) con chiavi a 256-bit, uno standard industriale per la crittografia sicura.

Padova, 05/07/2021

# CONFIGURAZIONE LEGALDOC
## AMBIENTE DI PRODUZIONE

# 1. Dati di configurazione del servizio

| | |
|---|---|
| Ragione sociale: | CONSIGLIO REGIONALE DEL LAZIO |
| Id bucket: | B54726 |
| Codice account: | JFLLD1 |
| Casella posta certificata: | supporto@cert.consreglazio.it |
| Data attivazione: | 09/03/2017 |

# 2. User associate

## 2.1. JFLLF01

Accesso: Abilitato
Tipo di accesso: WebServices + Interfaccia
Viewer: Sola lettura
Impronta: Lettura e creazione

**Tipologie documentali:**

| Tipologia documentale | Download | Conserva | Rettifica | Elimina | Ricerca |
|---|---|---|---|---|---|
| apau501194 | SI | SI | SI | SI | SI |
| atti501194 | SI | SI | SI | SI | SI |
| cad_regprot | SI | SI | SI | SI | SI |
| cont501194 | SI | SI | SI | SI | SI |
| paco501194 | SI | SI | SI | SI | SI |
| pec501194 | SI | SI | SI | SI | SI |

## 2.2. YYI9352

Accesso: Abilitato
Tipo di accesso: WebServices + Interfaccia
Viewer: Sola lettura
Impronta: Lettura e creazione

**Tipologie documentali:**

| Tipologia documentale | Download | Conserva | Rettifica | Elimina | Ricerca |
|---|---|---|---|---|---|
| apau501194 | SI | SI | SI | SI | SI |
| atti501194 | SI | SI | SI | SI | SI |
| cont501194 | SI | SI | SI | SI | SI |
| paco501194 | SI | SI | SI | SI | SI |
| pec501194 | SI | SI | SI | SI | SI |

## 2.3. JFLLF04

Accesso: Abilitato
Tipo di accesso: WebServices + Interfaccia
Viewer: Sola lettura
Impronta: Lettura e creazione

**Tipologie documentali:**

| Tipologia documentale | Download | Conserva | Rettifica | Elimina | Ricerca |
|---|---|---|---|---|---|
| cont501194 | SI | SI | SI | SI | SI |

## 2.4. JFLLF02

Accesso: Abilitato
Tipo di accesso: WebServices + Interfaccia
Viewer: Sola lettura
Impronta: Lettura e creazione

**Tipologie documentali:**

| Tipologia documentale | Download | Conserva | Rettifica | Elimina | Ricerca |
|---|---|---|---|---|---|
| apau501194 | SI | SI | SI | SI | SI |
| atti501194 | SI | SI | SI | SI | SI |
| paco501194 | SI | SI | SI | SI | SI |

## 2.5. JFLLF03

Accesso: Abilitato
Tipo di accesso: WebServices + Interfaccia
Viewer: Sola lettura
Impronta: Lettura e creazione

**Tipologie documentali:**

| Tipologia documentale | Download | Conserva | Rettifica | Elimina | Ricerca |
|---|---|---|---|---|---|
| paco501194 | SI | SI | SI | SI | SI |

## 2.6. JFLLF05

Accesso: Abilitato
Tipo di accesso: WebServices + Interfaccia
Viewer: Sola lettura

Impronta: Lettura e creazione

**Tipologie documentali:**

| Tipologia documentale | Download | Conserva | Rettifica | Elimina | Ricerca |
|---|---|---|---|---|---|
| apau501194 | NO | NO | NO | NO | NO |
| atti501194 | NO | NO | NO | NO | NO |
| cad_regprot | SI | SI | SI | SI | SI |
| cont501194 | NO | NO | NO | NO | NO |
| paco501194 | NO | NO | NO | NO | NO |
| pec501194 | NO | NO | NO | NO | NO |

## 2.7. YYE4668

Accesso: Abilitato
Tipo di accesso: WebServices + Interfaccia
Viewer: Sola lettura
Impronta: Lettura e creazione

**Tipologie documentali:**

| Tipologia documentale | Download | Conserva | Rettifica | Elimina | Ricerca |
|---|---|---|---|---|---|
| apau501194 | SI | SI | SI | SI | SI |
| atti501194 | SI | SI | SI | SI | SI |
| cad_regprot | SI | SI | SI | SI | SI |
| cont501194 | SI | SI | SI | SI | SI |
| paco501194 | SI | SI | SI | SI | SI |
| pec501194 | SI | SI | SI | SI | SI |

# 3. Policy associate

## 3.1. P54630 - Policy standard

### Formati di file ammessi alla conservazione:

| File Mime | Descrizione |
|---|---|
| application/pdf;NA | PDF |
| application/pkcs7;NA\|application/pdf;NA | PDF firmato |
| application/pkcs7;NA\|image/tiff;NA | TIFF firmato |
| application/pkcs7;NA\|text/plain;NA | TXT firmato |
| application/pkcs7;NA\|text/xml;1.0 | XML firmato |
| application/timestamp-reply;NA\|application/pdf;NA | PDF marcato |
| application/timestamp-reply;NA\|application/pkcs7;NA\|application/pdf;NA | PDF firmato e marcato |
| application/timestamp-reply;NA\|application/pkcs7;NA\|image/tiff;NA | TIFF firmato e marcato |
| application/timestamp-reply;NA\|application/pkcs7;NA\|text/plain;NA | TXT firmato e marcato |
| application/timestamp-reply;NA\|application/pkcs7;NA\|text/xml;1.0 | XML firmato e marcato |
| application/timestamp-reply;NA\|text/xml;1.0 | XML marcato |
| image/tiff;NA | TIFF |
| message/rfc822;NA | EML |
| text/plain;NA | TXT |
| text/xml;1.0 | XML |

### Formati di file indice ammessi:

| File Mime | Descrizione |
|---|---|
| text/xml;1.0 | XML |

### Tipologie documentali:

| Nome | Descrizione | Controllo |
|---|---|---|
| cont501194 | Contratti | nessuno |
| paco501194 | Pareri delle Commissioni | nessuno |
| apau501194 | Testo Approvato in Aula | nessuno |
| pec501194 | pec501194 | nessuno |
| atti501194 | Atti di Giunta | nessuno |
| cad_regprot | Registro di protocollo | nessuno |

**Firmatario:**
Nessun firmatario associato.

# 4. Campi di indice e controlli predefiniti per le Tipologie documentali

## 4.1. CONTRATTI - cont501194

| Label | Indice | Controllo obbligatorietà | Controllo numerazione | Controllo continuità numerazione rispetto a |
|---|---|---|---|---|
| 2 Data | data_documento_dt | SI | NO | - |
| 12 allegato | allegato_s | NO | NO | - |
| 11 annotazioni | annotazioni_s | SI | NO | - |
| 5 controparte | controparte_s | SI | NO | - |
| 8 data registrazione | data_reg_dt | NO | NO | - |
| 7 importo | importo_s | SI | NO | - |
| 10 imposta reg | imposta_reg_s | NO | NO | - |
| 3 natura | natura_s | SI | NO | - |
| 9 numero reg | numero_reg_s | NO | NO | - |
| 1 numero | numero_s | SI | NO | - |
| 6 oggetto | oggetto_s | SI | NO | - |
| 4 parte | parte_s | SI | NO | - |

## 4.2. PARERI DELLE COMMISSIONI - paco501194

| Label | Indice | Controllo obbligatorietà | Controllo numerazione | Controllo continuità numerazione rispetto a |
|---|---|---|---|---|
| Data documento | data_documento_dt | SI | NO | - |
| Codice identificativo amministrazione | codice_amm_s | NO | NO | - |
| Codice identificativo area organizzativa omogenea | codice_aoo_s | NO | NO | - |
| Data di protocollo secondo il formato individuato in base alle previsioni di cui art. 18 secondo comma del presente decreto | data_protocollo_dt | NO | NO | - |
| destinatario | destinatario_s | SI | NO | - |
| mittente | mittente_s | SI | NO | - |
| Progressivo di protocollo secondo il formato specifico dell'art. 8 del decreto del Presidente della Repubblica n.428 1998 | n_protocollo_s | NO | NO | - |
| Numero | numero_s | SI | NO | - |
| Oggetto | oggetto_s | SI | NO | - |
| Tipo Atto | tipo_atto_s | SI | NO | - |

## 4.3. TESTO APPROVATO IN AULA - apau501194

| Label | Indice | Controllo obbligatorietà | Controllo numerazione | Controllo continuità numerazione rispetto a |
|---|---|---|---|---|
| Data documento | data_documento_dt | SI | NO | - |
| Codice identificativo amministrazione | codice_amm_s | NO | NO | - |
| Codice identificativo darea organizzativa omogenea | codice_aoo_s | NO | NO | - |
| Data di protocollo secondo il formato individuato in base alle previsioni di cui art. 18 secondo comma del presente decreto | data_protocollo_dt | NO | NO | - |
| destinatario | destinatario_s | SI | NO | - |
| mittente | mittente_s | SI | NO | - |
| Progressivo di protocollo secondo il formato specifico dell'art. 8 del decreto del Presidente della Repubblica n.428 1998 | n_protocollo_s | NO | NO | - |
| Numero | numero_s | SI | NO | - |
| Oggetto | oggetto_s | SI | NO | - |
| Tipo Atto | tipo_atto_s | SI | NO | - |

## 4.4. PEC501194 - pec501194

| Label | Indice | Controllo obbligatorietà | Controllo numerazione | Controllo continuità numerazione rispetto a |
|---|---|---|---|---|
| Data documento | data_documento_dt | SI | NO | - |
| Destinatario | destinatario_s | SI | NO | - |
| Mittente | mittente_s | SI | NO | - |
| oggetto | oggetto_s | SI | NO | - |

## 4.5. ATTI DI GIUNTA - atti501194

| Label | Indice | Controllo obbligatorietà | Controllo numerazione | Controllo continuità numerazione rispetto a |
|---|---|---|---|---|
| Data documento | data_documento_dt | SI | NO | - |
| Codice identificativo amministrazione | codice_amm_s | NO | NO | - |
| Codice identificativo area organizzativa omogenea | codice_aoo_s | NO | NO | - |
| Data di protocollo secondo il formato individuato in base alle previsioni di cui art. 18 secondo comma del presente decreto | data_protocollo_dt | NO | NO | - |
| Destinatario | destinatario_s | SI | NO | - |
| Mittente | mittente_s | SI | NO | - |
| Progressivo di protocollo secondo il formato specifico dell'art. 8 del decreto del Presidente della Repubblica n.428 1998 | n_protocollo_s | NO | NO | - |
| Numero | numero_s | SI | NO | - |
| Oggetto | oggetto_s | SI | NO | - |
| Tipo Atto | tipo_atto_s | SI | NO | - |

## 4.6. REGISTRO DI PROTOCOLLO - cad_regprot

| Label | Indice | Controllo obbligatorietà | Controllo numerazione | Controllo continuità numerazione rispetto a |
|---|---|---|---|---|
| Data chiusura | data_documento_dt | SI | NO | - |
| Anno | anno_i | NO | NO | - |
| Codice fiscale soggetto prod | ccodice_fiscale_soggetto prod_s | NO | NO | - |
| Classificazione | classificazione_s | SI | NO | - |
| Codice identificativo Amministrazione | codice_amm_s | SI | NO | - |
| Codice identificativo AOO | codice_aoo_s | SI | NO | - |
| Codice fiscale destinatario | codice_fiscale_destinatario_s | NO | NO | - |
| Codice fiscale responsabile | codice_fiscale_responsabile_s | NO | NO | - |
| Codice fiscale soggetto prod 2 | codice_fiscale_soggetto prod_2_s | NO | NO | - |
| Data prima registrazione | data_prima_reg_dt | NO | NO | - |
| Denominazione Amministrazione | denominazione_amm_s | SI | NO | - |
| Destinatario | destinatario_s | NO | NO | - |

| Label | Indice | Controllo obbligatorietà | Controllo numerazione | Controllo continuità numerazione rispetto a |
|---|---|---|---|---|
| Codice identificativo del registro | id_registro_s | NO | NO | - |
| Note | note_s | NO | NO | - |
| Oggetto | oggetto_s | SI | NO | - |
| Numero progressivo del registro | progr_registro_i | NO | NO | - |
| Numero fine | prot_fine_i | SI | NO | - |
| Numero inizio | prot_inizio_i | SI | NO | - |
| Responsabile | responsabile_s | SI | NO | - |
| Soggetto produttore 2 | soggetto_prod_2_s | NO | NO | - |
| Soggetto produttore | soggetto_prod_s | SI | NO | - |

CONSIGLIO
REGIONALE
DEL LAZIO



# Piano della Sicurezza dei Sistemi di Gestione Informatica dei documenti del Consiglio regionale del Lazio

# PIANO DELLA SICUREZZA DEI SISTEMI DI GESTIONE INFORMATICA DEI DOCUMENTI DEL CONSIGLIO REGIONALE DEL LAZIO

**Premessa**

Il presente "Piano della sicurezza dei sistemi di gestione informatica dei documenti" (d'ora in poi Piano) relativo al sistema di gestione del flusso documentale e protocollo informatico e al sistema amministrativo contabile riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, che sono conservati presso il Data Center di Regione Lazio, via Rosa Raimondi Garibaldi, 7 – 00145 Roma e gestito da LAZIOcrea S.p.A.

Il piano fa riferimento agli applicativi riguardanti il sistema amministrativo contabile e quello del protocollo informatico e la gestione dei flussi documentali (di seguito, ove non diversamente specificato, sistemi di gestione informatica dei documenti), erogato in modalità ASP.

Per servizio ASP ("Application Service Providing" ossia "Fornitore di Servizi Applicativi") si intende la modalità con cui LAZIOcrea S.p.A. fornisce i servizi applicativi inerenti alle funzionalità gestite dal proprio software da remoto (attraverso un Data Center) in favore dei Clienti che vi accedono attraverso browser. Per Data Center si intende il centro servizi che ospita e gestisce l'insieme delle risorse hardware, il software di base, l'applicativo necessario a consentire l'utilizzo dei prodotti, dei software e delle procedure informatiche di proprietà di LAZIOcrea S.p.A., nonché i dati del Cliente.

Il Data Center di Regione Lazio è certificato in base agli standard internazionali ISO/IEC 27001:2013.

Il Consiglio regionale del Lazio contribuisce, attraverso le proprie misure e politiche di sicurezza, a stabilire adeguati livelli di salvaguardia dei documenti trattati.

Il piano in argomento è soggetto a revisione formale con cadenza almeno biennale.

I suddetti applicativi sono intregrati per le funzioni di autenticazione con l'Active Directory Regionale (dominio interno.regione.lazio.it) dove sono definite tutte le utenze nominative del personale del Consiglio Regionale.



## 1. Obiettivi del Piano di sicurezza dei sistemi di gestione informatica dei documenti

Il Piano di sicurezza dei sistemi di gestione informatica dei documenti garantisce che:

1. i documenti, gli atti e le informazioni trattati dall'Amministrazione siano disponibili, integri e riservati;
2. le categorie particolari di dati personali e i dati personali relativi a condanne penali e reati, *ex* artt. 9 e 10, del Regolamento generale sulla protezione dei dati (GDPR) UE/2016/679 vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

## 2. Generalità

L'Ente ha adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni.

Le misure adottate per la sicurezza sono le seguenti:

1. protezione dei sistemi di accesso e tutela delle informazioni;
2. assegnazione a ciascun utente dei sistemi di gestione informatica dei documenti, di una credenziale di identificazione personale (user ID), di una credenziale riservata di autenticazione (password) e di un profilo di autorizzazioni;
3. accesso ai sistemi di gestione informatica dei documenti avviene tramite credenziali di dominio;
4. cambio delle password con frequenza almeno trimestrale durante la fase di esercizio;
5. piano di continuità del servizio, con riferimento sia all'esecuzione che alla gestione delle copie di riserva dei dati e dei documenti (da effettuarsi con frequenza giornaliera), sia alla capacità di ripristino del sistema informativo entro il più breve tempo possibile in caso di disastro affidata al gestore del Data Center;
6. conservazione delle copie di riserva dei dati e dei documenti affidata al gestore del Data Center;
7. impiego e manutenzione di adeguati sistemi di sicurezza (antivirus, firewall, packaging di patch e service pack correttivi dei sistemi operativi);
8. impiego di un sistema di abilitazioni delle utenze alle funzionalità dell'applicativo, che consentano la trattazione delle registrazioni dei documenti esclusivamente a chi ne sia autore o assegnatario, in termini di:
    - visibilità delle registrazioni e dei dati,
    - gestione delle registrazioni,
    - visibilità e gestione degli allegati alle registrazioni;
9. archiviazione giornaliera immodificabile delle estrazioni in PDF/A del registro di protocollo;
10. accessibilità dei sistemi di gestione informatica dei documenti solo da intranet aziendale o da VPN con doppio fattore di autenticazione.

I dati personali registrati nel log dei sistemi operativi, del sistema di controllo degli accessi e delle operazioni svolte con i sistemi di gestione informatica dei documenti utilizzati saranno consultati, solo in caso di necessità, dal Responsabile di ciascun sistema per l'Ente e dal titolare dei dati e, ove previsto, da tutti gli aventi diritto in base alla Legge.

## 3. Formazione dei documenti: aspetti attinenti alla sicurezza

Nell'ambito di gestione dei sistemi informatici dei documenti, le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

1. l'identificabilità del soggetto che ha formato il documento, l'AOO di riferimento per i documenti soggetti a protocollazione;
2. quando prescritta, la sottoscrizione dei documenti informatici con firma digitale, ai sensi delle vigenti norme;

3. l'idoneità dei documenti a essere gestiti mediante strumenti informatici e a essere registrati mediante i relativi sistemi di gestione;
4. l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
5. la leggibilità dei documenti nel tempo e la loro conservazione;
6. l'interscambiabilità, per quanto riguarda il sistema di gestione del flusso documentale, dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *text editor* che adottano i formati standard previsti dalla normativa vigente in materia di documenti informatici e che posseggano requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura.

I documenti informatici redatti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro eventuale sottoscrizione con firma digitale, nei formati standard (preferibilmente PDF e PDF/A), come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto, di norma, con firma digitale.

Per attribuire una data certa a un documento informatico prodotto all'interno della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui alle Linee Guida AGID (Linee Guida sulla formazione, gestione e conservazione dei documenti informatici).

## 4. Gestione dei documenti informatici

Il Consiglio regionale ha in esercizio due sistemi di gestione informatica dei documenti; uno relativo al protocollo informatico ed uno relativo agli atti contabili-amministrativi.

Il sistema di protocollo informatico:

1. garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
2. assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata, in uscita e interni;
3. consente il reperimento delle informazioni riguardanti i documenti registrati;
4. consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte degli utenti del sistema stesso; ciascun utente è, di norma, autorizzato ad accedere unicamente alle registrazioni di protocollo a lui assegnate o da lui effettuate (*vedi paragrafo 6.1*);
5. consente la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Il sistema di gestione degli atti contabili-amministrativi:

1. garantisce la disponibilità, la riservatezza e l'integrità dei documenti;
2. assicura la corretta e puntuale registrazione dei documenti;
3. consente il reperimento delle informazioni riguardanti i documenti registrati;

4. consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte degli utenti del sistema; ciascun utente è, di norma, autorizzato ad accedere unicamente alle registrazioni a lui assegnate o da lui effettuate (*vedi paragrafo 6.3*);
5. consente la corretta organizzazione dei documenti nell'ambito del sistema d'archivio adottato.

### *4.1. Componente organizzativa della sicurezza*

Considerata la particolare modalità di fruizione dei sistemi di gestione informatica dei documenti, gran parte delle funzioni/responsabilità di sicurezza sono demandate all'erogatore dei relativi servizi. La componente organizzativa della sicurezza connessa con la gestione degli stessi e della documentazione è relativa principalmente alle attività svolte presso il Data Center LAZIOcrea, nelle vesti di erogatore dei servizi in modalità ASP.

L'abilitazione all'utilizzo delle proprie credenziali di dominio regionale per l'accesso ai sistemi è gestito dagli uffici preposti ed è subordinato alla presentazione di una apposita richiesta, effettuata utilizzando la mail istituzionale, da parte del dirigente/responsabile dell'ufficio in cui il dipendente è incardinato; nella richiesta devono essere indicati il ruolo da assegnare al dipendente e eventuali altri permessi da attribuire allo stesso.

L'accesso alla rete può avvenire esclusivamente tramite un processo di autenticazione che prevede un nome utente ed una password.

La password di accesso:

- ha una validità di **90 giorni** passati i quali scade automaticamente;
- deve essere lunga almeno **dieci** caratteri;
- deve contenere almeno **tre** delle seguenti categorie di caratteri: **maiuscole, minuscole, numeri, simboli**;
- non può essere riutilizzata per almeno le **quattro modifiche successive**;
- non può contenere parti del proprio **nome**, **cognome**, od **username**;
- non può contenere parole d'uso comune **facilmente identificabili**.

Nome utente e password sono strettamente personali. L'utente è tenuto a:

- non comunicare a terzi la password
- non annotare la password su supporti posti in vicinanza della propria postazione di lavoro o comunque incustoditi.

In caso di assenza anche temporanea del personale incaricato del trattamento dei dati, sui PC devono essere chiuse le procedure di accesso ai dati o attivato il blocco attraverso lo screen saver con password.

Gli utenti autorizzati accedono alle risorse informative dell'Ente tramite diversi livelli di autenticazione, a seconda dei privilegi autorizzativi che vengono loro rilasciati.

La modalità di lavoro agile o di telelavoro è abilitata a seguito di specifici contratti tra l'Amministrazione ed il dipendente. L'ASP LAZIOcrea fornisce gli strumenti necessari per permettere agli utenti di effettuare connessioni sicure con il sistema dell'Ente.

L'accesso ai portali da remoto viene eseguito tramite la MFA (Multi-Factor Authentication).

I dipendenti devono necessariamente registrare il proprio account di dominio all'interno di un'applicazione che genera codici di accesso casuali (es. Microsoft Authenticator, Google Authenticator). Questa registrazione permetterà di effettuare l'MFA (username, password ed un token univoco generato casualmente dall'app Authenticator) necessaria per accedere al portale extranet di Regione Lazio. Una volta effettuato l'accesso i dipendenti avranno a disposizione i link di collegamento alle risorse informative dove sarà possibile collegarsi mediante la propria utenza di dominio.

Nella gestione del Data Center sono state individuate tutte le figure preposte all'adozione di tutte le procedure di sicurezza previste nell'ambito dell'organigramma gestito per la certificazione ISO/IEC 27001:2013.

Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

1. *sicurezza informatica* - principalmente inerente alla definizione dei piani di sicurezza e della progettazione dei sistemi di sicurezza;
2. *sicurezza operativa* - realizza, gestisce e mantiene in efficienza le misure di sicurezza così da soddisfare le linee strategiche di indirizzo definite dalla funzione *sicurezza informatica;*
3. *revisione* - controlla le misure di sicurezza adottate, verificandone l'efficacia e la coerenza con le politiche di sicurezza.

Relativamente alla componente fisica della sicurezza sono stati definiti i ruoli previsti dalla certificazione ISO/IEC 27001:2013 per il Data Center di Regione Lazio.

La componente organizzativa della sicurezza afferente l'Ente è articolata e gestita secondo quanto stabilito dalla struttura competente dalla politica di sicurezza messa in atto dallo stesso.

### *4.2. Componente fisica della sicurezza*

Relativamente alla sicurezza fisica, il sistema si avvale del Data Center LAZIOcrea dotato di sistemi di protezione contro ogni minaccia, per garantire la massima sicurezza a dati e servizi. Il servizio di erogazione del Data Center è certificato ISO/IEC 27001:2013, e nello specifico:

1. per quanto riguarda la rete elettrica e refrigerazione: si avvale di un impianto di distribuzione elettrica ridondato; di gruppi di continuità statici (UPS); di un impianto di condizionamento dotato di 2 centrali frigorifere; di un sistema di controllo automatico;
2. per quanto riguarda la prevenzione incendi: si avvale di rilevamento fumi con sensori ottici analogici, doppie porte antincendio; spegnimento automatico incendi a gas inerte;
3. per quanto riguarda il controllo accessi: si avvale di sorveglianza armata; videocontrollo; sistema antintrusione; controllo accessi con lettore card e finger print.

### *4.3. Componente logica della sicurezza*

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Tale componente è stata realizzata attraverso:

1. l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto dannoso delle minacce sulle vulnerabilità del sistema informatico:
   a) identificazione, autenticazione ed autorizzazione degli utenti;
   b) riservatezza dei dati;

c) integrità dei dati;
d) integrità del flusso dei messaggi;
e) non ripudio dell'origine (da parte del mittente);
f) non ripudio della ricezione (da parte del destinatario);

2. la ridondanza dei sistemi di esercizio.

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità dei sistemi qui descritti, è stata implementata una soluzione centralizzata per la gestione degli utenti. Tale soluzione consente l'identificazione, l'autenticazione e l'autorizzazione degli utenti con le seguenti caratteristiche:

1. unico *login* per la gestione dei diritti di accesso ai servizi applicativi;
2. unico sistema di *repository* delle credenziali di accesso degli utenti;
3. unico database delle anagrafiche contenente tutti i profili di utenza.

### *4.4. Componente infrastrutturale della sicurezza*

Come già citato nel precedente paragrafo 4.2, nel Data Center sono disponibili i seguenti impianti, atti a garantire la sicurezza fisica dei dati:

1. antincendio
2. rilevazione dell'allagamento
3. luci di emergenza
4. continuità elettrica
5. controllo degli accessi e dei varchi fisici
6. gruppo di continuità (UPS) dimensionato
7. gruppo elettrogeno centralizzato

Gli impianti e le considerazioni precedenti valgono anche per la componente infrastrutturale relativa agli applicativi.

### *4.5. Gestione delle registrazioni e di sicurezza*

Le registrazioni di sicurezza sono costituite dalle informazioni di qualsiasi tipo (dati, transazioni, registrazioni, ecc.) presenti o transitate sui sistemi e che occorre mantenere dal punto di vista regolamentare, oppure necessarie in caso di indagini giudiziarie e dispute legali che abbiano come oggetto di contesa le operazioni effettuate sul sistema stesso o indispensabili per poter analizzare compiutamente lo svolgersi di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite da:

1. i log di sistema, generati dal sistema operativo;
2. i log dei dispositivi di protezione periferica del sistema informatico (intrusion detection system IDS, sensori di rete e firewall);
3. le registrazioni del sistema;

Le registrazioni di sicurezza sono soggette alle misure di sicurezza previste dalla certificazione ISO/IEC 27001:2013.

## 5. Trasmissione e interscambio dei documenti informatici

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono diffondere il contenuto della corrispondenza telematica, né duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sui contenuti stessi della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati e i documenti trasmessi sono conservati per il tempo necessario al perseguimento delle finalità per cui sono stati raccolti e trattati ai sensi del Regolamento UE 2016/679 e del decreto legislativo del 30 giugno 2003, n. 196 e successive modifiche.

Il server di posta elettronica certificata del fornitore esterno (*provider*) di cui si avvale l'AOO, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

1. accesso all'indice dei gestori di posta elettronica certificata, allo scopo di verificare l'integrità del messaggio e del suo contenuto;
2. tracciamento delle attività nel file di log della posta;
3. gestione automatica delle ricevute di ritorno.

Si precisa che il sistema amministrativo contabile non utilizza PEC di fornitori esterni ma solo server di posta di LAZIOcrea.

### *5.1.All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)*

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività e i processi amministrativi conseguenti (articolo 55, comma 4, DPR 445/2000).

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete.

Il mezzo di comunicazione telematica di base è la posta elettronica certificata del *provider* con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dal Codice dell'Amministrazione Digitale.

### *5.2.All'interno della AOO*

Per i messaggi scambiati all'interno della AOO con la posta elettronica (e quindi esterni al sistema di protocollo informatico) non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.

Gli uffici organizzativi di riferimento dell'AOO agiscono mediante strumenti informatici e telematici, nei rapporti interni.

## 6. Accesso ai documenti informatici

II controllo degli accessi è assicurato utilizzando le credenziali di accesso, personale *(userID)* e privata *(password)* e un sistema basato sull'assegnazione delle necessarie autorizzazioni agli utenti.

Tali autorizzazioni comprendono:

- *consultazione*;
- *inserimento;*
- *modifica;*
- *annullamento.*

I sistemi di gestione informatica dei documenti:

1. consentono il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti;
2. assicurano il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema, viene associata una *Access Control List* (ACL) che consente di stabilire quali utenti o gruppi di utenti hanno accesso a esso (sistema di autorizzazione o profilazione utenza).

Considerato che il sistema di norma segue la logica dell'organizzazione, ciascun utente può accedere solamente ai documenti che sono stati assegnati alla struttura di appartenenza.

Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso.

### *6.1. Utenti interni alla AOO*

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione del flusso documentale, sono attribuiti dalla Posizione Organizzativa del Protocollo Generale su richiesta del Direttore/Dirigente della struttura di appartenenza dell'utente. Tali livelli si distinguono in:

- abilitazione alla consultazione,
- abilitazione all'inserimento,
- abilitazione alla cancellazione e alla modifica delle informazioni.

I livelli di autorizzazione per l'accesso alle funzioni del sistema amministrativo contabile, sono attribuiti da LAZIOcrea su richiesta del Direttore/Dirigente della struttura di appartenenza dell'utente o dal riferimento individuato dal Consiglio e comunicato a LAZIOcrea come punto di interfaccia per le richieste di autorizzazioni all'accesso al sistema stesso. Tali livelli si distinguono in:

- abilitazione alla consultazione,
- abilitazione all'inserimento,
- abilitazione alla cancellazione e alla modifica delle informazioni.

La gestione delle utenze rispetta i seguenti principi operativi:

1. gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati;

2. la credenziale privata degli utenti non transita in chiaro sulla rete, né al momento della prima generazione, né successivamente al momento del login.

### *6.2. Accesso al registro di protocollo per utenti interni alla AOO*

L'accesso al registro di protocollo è regolato tramite le seguenti modalità:

1. assegnazione del documento alla struttura di competenza;
2. definizione delle ACL;
3. ruoli assegnati agli utenti;
4. registrazione "sensibile o riservata".

La visibilità completa sul registro di protocollo è consentita agli utenti abilitati. Più in generale, gli utenti abilitati a vedere tutte le registrazioni di protocollo sono quegli utenti per i quali, tra le abilitazioni di struttura organizzativa, sia stata definita la possibilità di visibilità su documenti e fascicoli.

L'utente assegnatario dei documenti protocollati è invece abilitato a una vista parziale sul registro di protocollo. Tale vista è definita da assegnazione e ACL.

### *6.3. Accesso al sistema di gestione amministrativo contabile per utenti interni*

L'accesso al sistema avviene tramite le seguenti modalità:

1. predisposizione dell'atto da parte dei soggetti coinvolti nell'elaborazione dello stesso;
2. definizione delle ACL;
3. ruoli assegnati agli utenti;
4. oscuramento dati/documenti sensibili.

La visibilità completa sul sistema è consentita agli utenti abilitati. Più in generale, gli utenti abilitati a vedere tutti gli atti sono quegli utenti per i quali, tra le abilitazioni di struttura organizzativa, sia stata definita la possibilità di visibilità sugli atti.

## 7. Conservazione dei documenti informatici

La conservazione dei documenti informatici avviene sulla base delle disposizioni riportate nelle "Linee guida sulla formazione, gestione e conservazione dei documenti informatici" emanate dall'AGID, garantendone l'immodificabilità del contenuto. Le modalità di invio in conservazione sono descritte nel Manuale di Conservazione.

## 8. Violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 2016/679 (data breach)

I provvedimenti di designazione del conservatore/responsabile esterno, redatti ai sensi dell'art. 28 del Regolamento UE 2016/679, contengono gli obblighi a carico di quest'ultimi del rispetto delle misure di sicurezza informatica e in modo particolare della procedura per la gestione delle violazioni dei dati personali.

Nello specifico si riportano di seguito la descrizione testuale delle procedure previste nei rispettivi provvedimenti in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 2016/679 (*data breach*):

- Sistemi informativi (ivi compresi siti e piattaforme informatiche) – Laziocrea S.p.A.

**Notifica di una violazione dei dati personali**

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del regolamento (UE) 2016/679 tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

**9.1 Violazione riguardante dati trattati dal titolare del trattamento**

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento, assiste il titolare del trattamento:

b) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, (a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);

c) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679 devono essere indicate nella notifica del titolare del trattamento e includere almeno:

i) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

ii) le probabili conseguenze della violazione dei dati personali;

iii) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

d) nell'adempiere, in conformità dell'articolo 34 del regolamento (UE) 2016/679 all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

**9.5 Violazione riguardante dati trattati dal responsabile del trattamento**

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:

f) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);

g) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
h) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'allegato III tutti gli altri elementi che il responsabile del trattamento è tenuto a fornire quando assiste il titolare del trattamento nell'adempimento degli obblighi che incombono al titolare del trattamento a norma degli articoli 33 e 34 del regolamento (UE) 2016/679.

(*clausola 9 dell'annesso al contratto prot.0017321 del 29.07.2022*)

- Servizi di posta elettronica certificata (PEC) – Infocert S.p.A.

Il Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento si impegna a supportare il Titolare nell'ambito di tale attività.

(*punto 12 Contratto attuativo nell'ambito della convenzione per servizi di posta elettronica Certificata (PEC) – Nomina responsabile del trattamento dei dati*).

- Servizio di conservazione – PArER - Regione Emilia-Romagna

**11. Violazione dei dati personali e obblighi di notifica**

11.1 - Il Responsabile del trattamento, in virtù di quanto previsto dall'art. 33 del Regolamento e nei limiti di cui al perimetro delle attività affidate, deve comunicare a mezzo di posta elettronica certificata all'Ente produttore nel minor tempo possibile, e comunque non oltre 24 (ventiquattro) ore da quando ne abbia avuto notizia, qualsiasi violazione di sicurezza che abbia comportato accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, ivi incluse quelle che abbiano riguardato i propri sub-Fornitori. Tale comunicazione deve contenere ogni informazione utile alla gestione del *data breach*, oltre a:

a) descrivere la natura della violazione dei dati personali
b) le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
c) i recapiti del DPO nominato o del soggetto competente alla gestione del *data breach*;
d) la descrizione delle probabili conseguenze della violazione dei dati personali;
e) una descrizione delle misure adottate o che si intende adottare per affrontare la Violazione della sicurezza, compreso, ove opportuno, misure per mitigare i suoi possibili effetti negativi.

11.2 - Il Responsabile del trattamento deve fornire tutto il supporto necessario all'Ente produttore ai fini delle indagini e sulle valutazioni in ordine alla violazione di dati, anche al fine di individuare, prevenire e limitare gli effetti negativi della stessa, conformemente ai suoi obblighi ai sensi del

presente articolo e, previo accordo con l'Ente produttore, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa. Il Responsabile del trattamento non deve rilasciare, né pubblicare alcun comunicato stampa o relazione riguardante eventuali data breach o violazioni di trattamento senza aver ottenuto il previo consenso scritto dell'Ente produttore.
(*Punto 11, Allegato 1 "Accordo di collaborazione per lo svolgimento della funzione di Conservazione dei documenti informatici - Deliberazione Giunta n. 484 del 27/07/2021*).

Servizio di conservazione – Infocert S.p.A.

Con particolare riferimento agli obblighi in materia di notificazione dei dati personali ex artt. 33 e 34 del Regolamento, informare il Titolare (o, ove necessario o richiesto, il Titolare dell'oggetto della conservazione) della eventuale violazione di dati personali senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione stessa.
(*Affidamento del procedimento di conservazione Servizio Legaldoc - Nomina del responsabile del trattamento dei dati personali, ai sensi del Regolamento UE n. 679/2016*).